SIEMENS

SIMATIC NET

GPRS/GSM-Modem SINAUT MD740-1

Systemhandbuch

Vorwort, Inhaltsverzeichnis

Einleitung **1**

Die LEDs des MD740-1 **2**

Inbetriebnahme **3**

Konfiguration **4**

Integrierte Website zeigt Geräte- und Verbindungsdaten **5**

Firmware-Update und Recovery **6**

Technische Daten **7**

Glossar

C79000-G8900-C212

Ausgabe 11/2006

Sicherheitshinweise

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.



Gefahr

bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.



Warnung

bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.



Vorsicht

mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Vorsicht

ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Achtung

bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zugehörige Gerät/System darf nur in Verbindung mit dieser Dokumentation eingerichtet und betrieben werden. Inbetriebsetzung und Betrieb eines Gerätes/Systems dürfen nur von **qualifiziertem Personal** vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieser Dokumentation sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Bestimmungsgemäßer Gebrauch

Beachten Sie Folgendes:



Warnung

Das Gerät darf nur für die im Katalog und in der technischen Beschreibung vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Fremdgeräten und -komponenten verwendet werden. Der einwandfreie und sichere Betrieb des Produktes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung und Montage sowie sorgfältige Bedienung und Instandhaltung voraus.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Automation and Drives
Postfach 48 48
90437 NÜRNBERG
DEUTSCHLAND

Dokumentbestell-Nr. C79000-G8900-C212-01
Ausgabe 04/2006

Allgemeine Hinweise zu dem Produkt

Das Produkt MD740-1 entspricht der europäischen Norm EN60950,05.2003, Einrichtungen der Informationstechnik - Sicherheit.
Lesen Sie vor Gebrauch des Gerätes die Installationsanleitung sorgfältig durch.
Halten Sie das Gerät von Kindern fern, besonders von Kleinkindern.
Das Gerät darf nicht im Freien oder in Feuchträumen installiert und betrieben werden.
Nehmen Sie das Gerät nicht in Betrieb, wenn Anschlussleitungen oder das Gerät selbst beschädigt sind.

Externe Stromversorgung

Verwenden Sie nur eine externe Stromversorgung die ebenfalls der EN60950 entspricht. Die Ausgangsspannung der externen Stromversorgung darf 30V DC nicht überschreiten. Der Ausgang der externen Stromversorgung muss kurzschlussfest sein.



Warnung

Das SINAUT MD740-1 darf nur aus Stromversorgungen nach IEC/EN60950 Abschnitt 2.5 "Stromquelle mit begrenzter Leistung" versorgt werden.

Die externe Stromversorgung für das SINAUT MD740-1 muss den Bestimmungen für NEC Klasse 2 Stromkreisen entsprechen, wie im National Electrical Code ® (ANSI/NFPA 70) festgelegt.

Bei Anschluss an eine Batterie oder einen Akkumulator beachten Sie, dass zwischen dem Gerät und der Batterie oder Akkumulator eine allpolige Trennvorrichtung (Batteriehauptschalter) mit ausreichendem Trennvermögen sowie eine Sicherung mit ausreichendem Trennvermögen vorzusehen sind (z. B. Pudenz FKS Sicherungssatz 32 V, 3 A, Best.-Nr. 162.6185.430).

Beachten Sie den Abschnitt *Technische Daten* dieser Dokumentation (Kapitel 7) sowie die Einbau- und Nutzungsvorschriften des jeweiligen Herstellers der Stromversorgung, der Batterie oder des Akkumulators.

SIM-Karte

Zur Installation der SIM-Karte muss das Gerät geöffnet werden. Trennen Sie das Gerät vor dem Öffnen von der Versorgungsspannung. Statische Aufladungen können das Gerät im geöffneten Zustand beschädigen. Entladen Sie die elektrische Aufladung Ihres Körpers vor dem Öffnen des Gerätes. Berühren Sie dazu eine geerdete Oberfläche, z.B. das Metallgehäuse des Schaltschrankes. Beachten Sie das Kapitel 3.3.

Umgang mit Kabeln

Ziehen Sie niemals einen Kabelstecker am Kabel aus seiner Buchse, sondern ziehen Sie am Stecker. Kabelstecker mit Schraubbefestigungen (D-Sub.) müssen immer fest angeschraubt werden. Führen Sie die Kabel nicht ohne Kantenschutz über scharfe Ecken und Kanten. Sorgen Sie gegebenenfalls für eine ausreichende Zugentlastung der Kabel.

Achten Sie bitte darauf, dass aus Sicherheitsgründen der Biegeradius der Kabel eingehalten wird.

Die Nichteinhaltung der Biegeradien des Antennenkabels führt zu Verschlechterung der Sende- und Empfangseigenschaften des Gerätes. Der minimale Biegeradius darf statisch den 5-fachen Kabeldurchmesser und dynamisch den 15fachen Kabeldurchmesser nicht unterschreiten.

Funkgerät



Warnung

Verwenden Sie das Gerät niemals in Bereichen, in denen der Betrieb von Funkeinrichtungen untersagt ist. Das Gerät enthält einen Funksender, der gegebenenfalls medizinische elektronische Geräte wie Hörgeräte oder Herzschrittmacher in ihrer Funktion beeinträchtigen kann. Ihr Arzt oder der Hersteller solcher Geräte können Sie beraten.

Damit keine Datenträger entmagnetisiert werden, lagern Sie bitte keine Disketten, Kreditkarten oder andere magnetische Datenträger in der Nähe des Gerätes.

Antennen-Montage



Warnung

Das Einhalten der empfohlenen Strahlungsgrenzwerte der Strahlenschutzkommission vom 13./14. September 2001 muss gewährleistet sein.

Montage einer Außenantenne

Vorsicht

Bei der Installation einer Antenne im Freien ist es zwingend erforderlich, dass die Antenne durch Fachpersonal fachgerecht montiert wird. Die Einhaltung der Blitzschutznorm VDE V 0185 Teil 1 bis 4 in ihrer aktuellen Fassung und weiterführende Normen sind dabei vorgeschrieben.

Die Gebäude-Blitzschutzklasse (SK)

Vorsicht

Bei der Außenmontage darf die Antenne nur innerhalb der Blitzschutzzonen O/E bzw. 1 angebracht werden. Diese Blitzschutzzonen werden durch den Blitzschutzkugelradius vorgegeben.

Das EMV Blitzschutzzonen-Konzept

Vorsicht

Das EMV Blitzschutzzonen-Konzept ist einzuhalten. Um große Induktionsschleifen zu vermeiden, ist ein Blitzschutz-Potentialausgleich anzuwenden. Wird die Antenne bzw. das Antennenkabel in der Nähe der Blitzschutzanlage montiert, müssen die Mindestabstände zur Blitzschutzanlage eingehalten werden. Ist dies nicht möglich, ist eine isolierte Montage wie in der Blitzschutznorm VDE V 0185 Teil 1 bis 4, in ihrer aktuellen Fassung beschrieben, zwingend erforderlich.

FCC Part 15

Aufgrund entsprechender Tests wurde befunden, dass dieses Gerät den Grenzwerten für digitale Geräte der Klasse A entspricht, gemäß der FCC Rules Part 15. Diese Grenzwerte sind so festgelegt, dass bei ihrer Einhaltung angemessener Schutz gegen schädliche und störende Interferenzen gewährleistet ist, wenn das betreffende Gerät im Wohnbereich installiert ist. Dieses Gerät erzeugt und benutzt Hochfrequenzen und kann diese ausstrahlen. Wenn dieses Gerät nicht in Übereinstimmung mit den Instruktionen installiert und benutzt wird, kann es störende Interferenzen für den Funkverkehr bewirken. Es kann jedoch nicht garantiert werden, dass es bei bestimmten Installationen, auch wenn diese in Übereinstimmung mit den Instruktionen vorgenommen werden, keine störenden Interferenzen geben kann. Falls dieses Gerät störende Interferenzen beim Radio- oder Fernsehempfang bewirkt, was durch Ein- und Ausschalten des Gerätes ermittelt werden kann, empfehlen wird dem Benutzer, folgende Gegenmaßnahmen zu ergreifen.

- Ändern Sie die Ausrichtung der Empfangsantenne oder installieren Sie diese an anderer Stelle.
- Vergrößern Sie den Abstand zwischen dem MD740-1 und dem Radio- oder Fernsehempfänger.
- Schließen Sie das Gerät an eine Netzsteckdose an, die sich in einem anderen Stromkreis befindet als die, an der der Empfänger angeschlossen ist.
- Wenden Sie sich an einen Fachhändler / Installateur oder an einen kompetenten Fachmann für TV und Radioempfang und fragen Sie ihn.

FCC Part 15.19

Dieses Gerät entspricht den Bestimmungen in Part 15 der FCC Rules. Sein Betrieb unterliegt folgenden Bedingungen:

1. Dieses Gerät bewirkt möglicherweise keine schädlichen oder störenden Interferenzen, und
2. dieses Gerät muss empfangene Interferenzen hinnehmen können, auch solche, die ein unerwünschtes Betriebsverhalten bewirken könnten.

FCC Part 15.21

Modifikationen am Gerät, denen dieser Hersteller nicht ausdrücklich zugestimmt hat, können dazu führen, dass der Benutzer nicht mehr befugt ist, das Gerät zu betreiben.

Installation nur durch Fachpersonal

Das SINAUT MD740-1 darf nur mit einer Antenne aus dem Zubehörsortiment des SINAUT MD740-1 betrieben werden.

Ausschließlich Fachpersonal darf das SINAUT MD740-1 und dessen Antenne installieren und warten. Bei Arbeiten an der Antenne oder bei Arbeiten näher als unten angegeben muss der Sender ausgeschaltet sein.

HF-Exposition

Vorsicht

Normalerweise arbeitet die am Sender dieses Gerätes angeschlossene Antenne in allen Richtungen mit 0 dB Verstärkung. Die Composite Power im PCS-Modus ist bei Benutzung dieser Antenne geringer als 1 Watt ERP.

Die mit diesem mobilen Gerät benutzen internen / externen Antennen müssen **mindestens 20 cm von Personen entfernt sein**. Und sie dürfen nicht so platziert oder betrieben werden, dass sie in Verbund mit einer anderen Antenne oder Sender arbeiten.

Vorsicht

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

Vorsicht GPRS Kosten

Bitte beachten Sie, dass auch beim (Wieder-) Aufbau einer Verbindung, bei Verbindungsversuchen zur Gegenstelle (z.B. Server ausgeschaltet, falsche Zieladresse, etc.) sowie zum Erhalt einer Verbindung kostenpflichtige Datenpakete ausgetauscht werden.

Firmware mit Open Source GPL/LGPL

Die Firmware von SINAUT MD740-1 enthält open Source Software unter GPL/LGPL Bedingungen. Gemäß des Abschnitts 3b von GPL und des Abschnitts 6b von LGPL bieten wir Ihnen den Sourcecode an. Bitte schreiben Sie an

s_opsource@gmx.net
s_opsource@gmx.de

Als Betrifftext Ihrer E-Mail geben Sie bitte 'Open Source MD740' an, um Ihre Nachricht leicht herausfiltern zu können. Die Liste der GPL/LGPL Software können Sie der readme-Datei entnehmen.

Firmware mit OpenBSD

Die Firmware von SINAUT MD740-1 enthält Teile aus der OpenBSD-Software. Die Verwendung von OpenBSD-Software verpflichtet zum Abdruck des folgenden Copyright-Vermerkes:

Vorwort

Zweck dieser Dokumentation

Diese Dokumentation begleitet Sie auf Ihrem Weg zum erfolgreichen Einsatz des GPRS/GSM-Modems SINAUT MD740-1. Sie führt verständlich und anschaulich in das Thema ein und gibt Ihnen eine Übersicht über das Einsatzgebiet der Hardware. Sie erläutert Ihnen, wie das Modem unter Berücksichtigung der Betriebsbedingungen in Betrieb genommen und konfiguriert wird. Die vorliegende Dokumentation zeigt die technischen Daten und die erfüllten Normen und Zulassungen für das GPRS/GSM-Modem MD740-1.

Gültigkeitsbereich der Dokumentation

Das vorliegende Handbuch ist abgestimmt auf folgende Produktversionen:

- GPRS/GSM-Modem MD740-1 Hardwareausgabestand 1.x

SIMATIC Technical Support

Sie erreichen den Technical Support für alle A&D-Produkte über

- Telefon: +49 (0) 180 5050 222
- Fax: +49 (0) 180 5050 223

Weitere Informationen zu unserem Technical Support finden Sie im Internet unter

http://www.siemens.com/automation/service

Service & Support im Internet

Zusätzlich zu unserem Dokumentations-Angebot bieten wir Ihnen im Internet unser komplettes Wissen online an:

http://www.siemens.com/automation/service&support

Dort finden Sie:

- Aktuelle Produkt-Informationen (Aktuelles), FAQs (Frequently Asked Questions), Downloads, Tipps und Tricks.
- Der Newsletter versorgt Sie ständig mit den aktuellsten Informationen zu Ihren Produkten.
- Der Knowledge Manager findet die richtigen Dokumente für Sie.
- Im Forum tauschen Anwender und Spezialisten weltweit Ihre Erfahrungen aus.
- Finden Sie Ihren Ansprechpartner für Automation & Drives vor Ort über unsere Ansprechpartner-Datenbank.
- Informationen über Vor-Ort-Service, Reparaturen, Ersatzteile und vieles mehr steht für Sie unter dem Begriff »Leitungen« bereit.

Die aktuellste Version dieser Dokumentation finden Sie unter der Beitrags-ID 22550242.

Haben Sie noch Fragen zur Nutzung der im Handbuch beschriebenen Produkte? Dann wenden Sie sich bitte an Ihren Siemens-Ansprechpartner in der für Sie zuständigen Vertretung oder Geschäftsstelle.

Die Adressen finden Sie an folgenden Stellen:

- Im Internet unter: http://www.siemens.com/automation/partner
- Im Internet unter: http://www.siemens.com/simatic-net
  speziell für SIMATIC NET-Produkte
- Im Katalog CA 01
- Im Katalog IK PI (speziell für SIMATIC NET-Produkte)

Trainingscenter SIMATIC

Um Ihnen den Einstieg zu erleichtern, bieten wir Ihnen entsprechende Kurse an. Wenden Sie sich bitte an Ihr regionales Trainingscenter oder an das zentrale Trainingscenter in

D-90327 Nürnberg

Telefon: +49 (911) 895-3200

http://www.sitrain.com

Trainingscenter SIMATIC NET

Speziell für Kurse für Produkte von SIMATIC NET wenden Sie sich bitte an:

SIEMENS AG

Siemens AG, A&D Informations- und Trainings-Center

Dynamostr. 4

D-68165 Mannheim

Telefon: +49 (621) 4 56-23 77

Fax: +49 (621) 4 56-32 68

Inhaltsverzeichnis

1 Einleitung 13

1.1 Überblick 13

1.2 Voraussetzungen für den Einsatz des MD740-1 16

1.3 IP-Adresse der Gegenstelle 17

2 Die LEDs des MD740-1 19

3 Inbetriebnahme 21

3.1 Gerät anschließen 22

3.2 PIN konfigurieren 24

3.3 SIM-Karte einlegen oder wechseln 25

4 Konfiguration 31

4.1 Übersicht 31

4.2 Menü Netzwerk 37

4.2.1 Netzwerk → Lokal 37

4.2.2 Netzwerk → GPRS 39

4.2.3 Netzwerk → Status 41

4.3 Menü Firewall 42

4.3.1 Firewall → Eingehend 43

4.3.2 Firewall → Ausgehend 45

4.3.3 Firewall → Port Weiterleitung 47

4.3.4 Firewall → NAT 49

4.3.5 Firewall → Erweiterte Einstellungen 51

4.3.6 Firewall → Logs 53

4.4 Menü VPN 54

4.4.1 VPN-Verbindungen 55

4.4.2 VPN → Maschinenzertifikat 69

4.4.3 VPN → Erweiterte Einstellungen 71

4.4.4 VPN → L2TP 73

4.4.5 VPN → IPsec Status 74

4.4.6 VPN → L2TP Status 76

4.4.7 VPN → VPN Logs 77

4.5 Menü Dienste 78

4.5.1 Dienste → DNS 78

4.5.2 Dienste → DynDNS Überwachung 80

4.5.3 Dienste → DynDNS (Anmelden) 81

4.5.4 Dienste → DHCP 83

4.5.5 Dienste → NTP 86

4.5.6 Dienste → Remote Logging 89

4.6 Menü-Zugang 91

4.6.1 Zugang → Passworte 91

4.6.2 Zugang → Sprache 93

4.6.3 Zugang → HTTPS 94

4.6.4 Zugang → SSH 97

4.7 Menü Features 100

4.7.1 Features → Installiere Update 100

4.7.2 Features → Update Server 102
4.7.3 Features → Softwareinformationen 103
4.7.4 Features → Hardwareinformationen 104
4.8 Menü Support 105
4.8.1 Support → Snapshot 105
4.8.2 Support → Status 106
4.9 Menü System 108
4.9.1 System → Konfigurations-Profile 108
4.9.2 System → Neustart 111
4.9.3 System → Logs 112
4.10 CIDR (Classless InterDomain Routing) 113
4.11 Netzwerkbeispiele 114

5 Integrierte Website zeigt Geräte- und Verbindungsdaten des Modem-Teils 117
5.1 Lokal über die Service-Schnittstelle auf den Web-Server des Modem-Teils zugreifen 118
5.2 Lokal über die Applikations-Schnittstelle (Buchse 10/100 BASE-T) auf den Web-Server des Modem-Teils zugreifen 121
5.3 Von einem entfernten Rechner aus über das GPRS-Netz auf den Web-Server des Modem-Teils des MD740-1 zugreifen 123
5.4 Die Website des MD740-1 124

6 Firmware-Update und Recovery 129
6.1 Update der Firmware des Modem-Teils 129
6.2 Recovery: Auf Werkseinstellungen zurücksetzen 130
6.3 Update der VPN-Software 131

7 Technische Daten 133

Glossar 137

Einleitung 1

1.1 Überblick

Das SINAUT MD740-1 stellt per GPRS (General Packet Radio Service) eines GSM-Netzes (Global System for Mobile Communication = Mobilfunknetz) eine gesicherte IP-Datenverbindung her.

Funktionen

Dazu vereinigt das Gerät folgende Funktionen:

- GPRS-Modem für die flexible Datenkommunikation per GPRS
- VPN-Router für sichere Datenübertragung über öffentliche Netze (IPSec Protokoll, 3DES-Datenverschlüsselung, AES Verschlüsselung)
- Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse (stateful packet inspection) und blockiert unerwünschten Datenverkehr (Anti-Spoofing)

Konfiguration

Die Konfiguration des Gerätes erfolgt einfach mit einem Web-Browser.

VPN-Features

Das SINAUT MD740-1 bietet folgende VPN-Features

- Protokoll: IPsec (Tunnel und Transport Mode)
- IPsec DES Verschlüsselung mit 56 Bit
- IPsec 3DES Verschlüsselung mit 168 Bit
- IPsec AES Verschlüsselung mit 128, 192 und 256 Bit

- Paket-Authentifizierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Quick Mode
- Authentisierung: Pre-Shared Key (PSK), X.509v3 Zertifikate
- DynDNS
- NAT-T
- Dead Peer Detection (DPD)

Firewall-Features

Das SINAUT MD740-1 bietet folgende Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- NAT (IP Masquerading)
- Port Forwarding

Weitere-Features

Das SINAUT MD740-1 bietet folgende weiteren Features

- DNS Cache
- DHCP Server
- NTP
- Remote Logging

Typische SINAUT-Anwendungsbeispiele

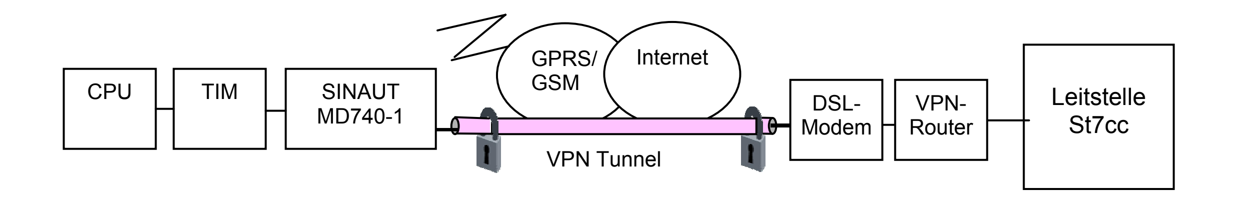


Abbildung 1-1 Verbindung zwischen CPU und Leitstelle

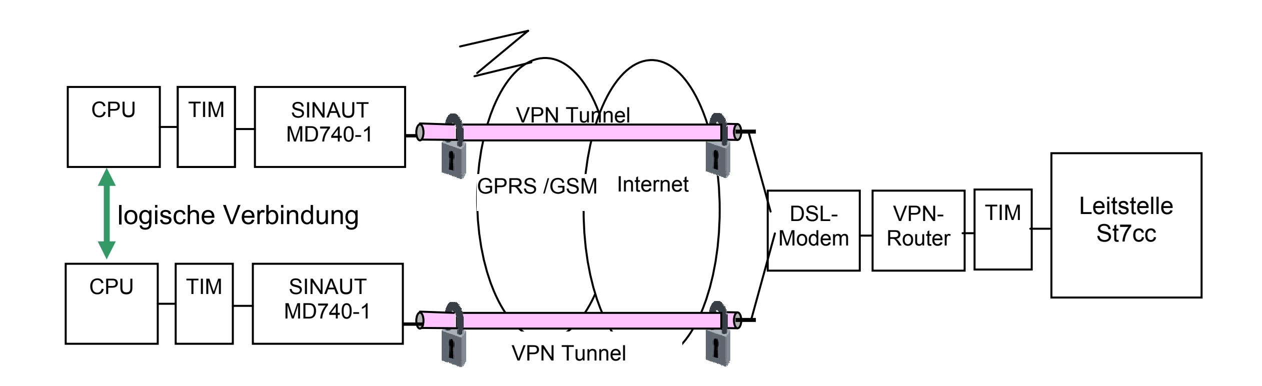


Abbildung 1-2 Verbindung zwischen zwei CPU

1.2 Voraussetzungen für den Einsatz des MD740-1

Um das MD740-1 einsetzen zu können, sind folgende Voraussetzungen erforderlich:

- Ein Teilnehmervertrag mit einem GSM-Netzbetreiber (z. B. T-Mobile, Vodafone, E-Plus, O2, Cingular), der GPRS unterstützt.
- Die Freischaltung des GPRS für den betreffenden Anwender durch den Netzbetreiber.

1.3 IP-Adresse der Gegenstelle

Damit ein MD740-1 aktiv eine VPN-Verbindung herstellen kann, muss die Gegenstelle eine feste IP-Adresse haben. (Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einen Punkt getrennt, z. B.: 255.122.201.115). Bei vielen Internet Service Providern (ISPs) werden die IP-Adressen jedoch dynamisch zugewiesen, d. h. die IP-Adressen der Rechner bzw. Netze, die Zugriff zum Internet haben, ändern sich. Zur Erlangung einer festen IP-Adresse gibt es folgende Möglichkeiten:

- Feste IP-Adresse durch Standleitung zum GPRS
- Feste IP-Adresse durch Internet Service Provider
- Fester DNS-Name über DynDNS-Service

Feste IP-Adresse durch Standleitung zum GPRS

Die Gegenstelle ist über eine gemietete Standleitung mit dem GPRS verbunden. Dann ist ihr vom Netzbetreiber in der Regel eine feste IP-Adresse zugeordnet worden.

Feste IP-Adresse durch Internet Service Provider

Die Gegenstelle ist über das Internet erreichbar, und ihr ist vom Internet Service Provider eine feste IP-Adresse zugeteilt. (Kann bei einigen Internet Service Providern beantragt werden.)

Fester DNS-Name über DynDNS-Service

Um die Problematik der dynamischen IP-Adressvergabe zu lösen, können DynDNS-Dienste genutzt werden. Durch einen solchen Dienst ist z. B. das MD740-1 oder die Gegenstelle, egal welche dynamische IP-Adresse sie im Moment besitzt, über einen festen Domain Namen zu erreichen. Bei jedem Wechsel der IP-Adresse meldet das MD740-1 bzw. die Gegenstelle die neue IP-Adresse dem DynDNS Server, so dass auf dem DNS-Server dem Domain Namen stets die aktuelle IP-Adresse zugeordnet ist - siehe *Glossar*. Beim Wechsel einer IP-Adresse kann allerdings eine Zeit von wenigen Minuten bis zu 1 Stunde vergehen, in der das Modem nicht erreichbar ist.

Die Nutzung eines DynDNS-Dienstes erfordert den Abschluss eines Vertrages mit einem entsprechenden Anbieter, z. B. DynDNS.org oder DNS4BIZ.com.

Die LEDs des MD740-1

2

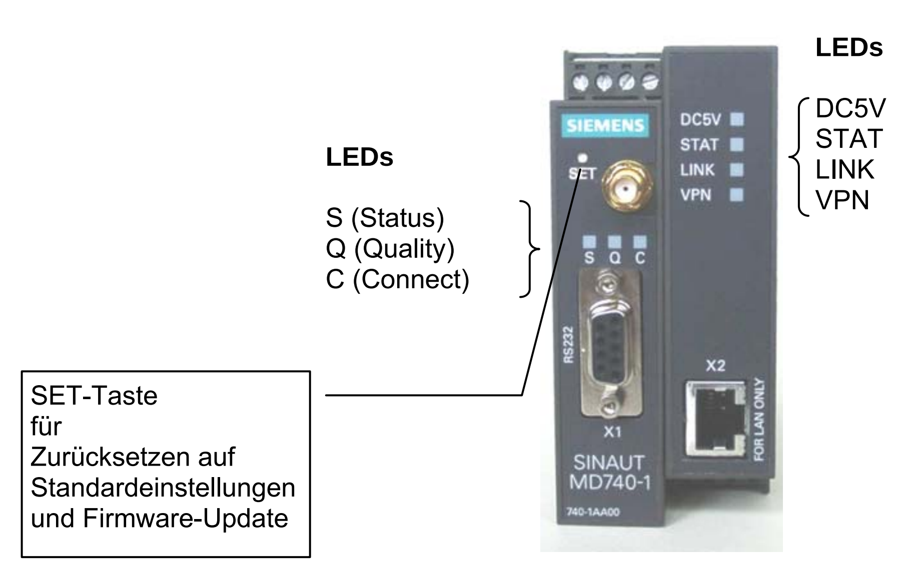


Abbildung 2-1 Die LEDs des MD740-1

LED	Farbe	Zustand	Bedeutung
DC5V	Grün	EIN	Gerät eingeschaltet, Betriebsspannung liegt an.
		AUS	Gerät ausgeschaltet, Betriebsspannung fehlt.
STAT	Grün	Blinkend	VPN-Board betriebsbereit.
LINK	Grün	EIN	Ethernet-Verbindung zum lokalen Rechner bzw. LAN hergestellt.
		AUS	Keine Ethernet-Verbindung zum lokalen Rechner bzw. LAN
VPN	Grün	EIN	VPN-Tunnel aufgebaut (siehe Hinweis).
		AUS	VPN-Tunnel nicht aufgebaut.

Tabelle 2-1 Bedeutung der DC5V, STAT, LINK, VPN LEDs

Hinweis

Kurz nach dem Einschalten des MD740-1 wird die LED VPN für kurze Zeit eingeschaltet, ohne dass der VPN-Tunnel aktiv ist. Ursache: Selbsttest der Komponenten beim Hochfahren des Gerätes.

S(Status), Q(Quality), C(Connect)

LED	Zustand	Bedeutung
S,Q,C gemeinsam	Schnelles Lauflicht	Booten
	Langsames Lauflicht	Update (siehe Hinweis 1)
	Synchrones schnelles Blinken	Error (Fehler)
S (Status)	Langsam blinkend	Warten auf PIN-Eingabe
	Schnell blinkend	PIN-Fehler / SIM-Fehler
	AUS	Keine GPRS Verbindung
	EIN	GPRS-Verbindung vorhanden
Q (Quality)	Langsam blinkend	Einbuchen ins GSM-Netz
	1 mal blinken mit Intervall	Feldstärke nicht ausreichend oder unbekannt (siehe Hinweis 2)
	2 mal blinken mit Intervall	Feldstärke ausreichend
	3 mal blinken mit Intervall	Feldstärke gut
	immer EIN	Feldstärke sehr gut
	AUS	Warten auf PIN
C (Connect)	AUS	Keine Verbindung
	EIN	Verbindung zur Gegenseite (bei GPRS: Authentifizierung und IP-Vergabe war erfolgreich.

Tabelle 2-2 Bedeutung der S, Q, C LEDs

Hinweise

1. Während eines Updates der Kommunikationssoftware wird zuerst ein langsames Lauflicht angezeigt. Im weiteren Verlauf ist nur noch die LED S im Zustand EIN.
2. Kurz nach dem Einbuchen wird die Feldstärke immer durch 1-maliges Blinken der Quality-LED als minimal bzw. unbekannt signalisiert. Ursache: Zu diesem Zeitpunkt hat das Gerät lediglich registriert, dass Feldstärke vorhanden ist. Die tatsächliche Ermittlung der Feldstärke erfolgt erst beim nächsten Check nach 15 Sekunden.

Inbetriebnahme

3

Überblick

Um das Gerät in Betrieb zu nehmen, führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

1. Gerät anschließen (siehe Kap. 3.1)

2. PIN Konfiguration ausführen (siehe Kap. 3.2)

Achtung

Geben Sie erst dem Gerät die PIN der SIM-Karte bekannt. Erst danach die SIM-Karte einlegen!

Das Gerät unterstützt auch SIM-Karten ohne PIN. Hat Ihre SIM-Karte keine PIN, können Sie die SIM-Karte auch vor der Konfiguration einlegen.

---

3. SIM Karte ins Gerät einlegen (siehe Kap. 3.3)

Vorsicht

Das Gerät muss ausgeschaltet sein, wenn Sie die SIM-Karte einlegen oder entnehmen.

---

4. Weitere Konfiguration durchführen (siehe Kap. 4)

3.1 Gerät anschließen

Stromversorgung

Die Schraubklemmen oben sind zum Anschließen der Stromversorgungsquelle: 24 V Gleichspannung (nominal); **I** typ. 360mA@24V; **I** max. 1A.



Abbildung 3-1

Nr.	Bedeutung
1	Die beide Schraubklemmen links **(+ 24 V)** sind miteinander verbunden.
2	Die beide Schraubklemmen rechts **(0 V)** sind miteinander verbunden.
3	Antenne (ca. 50 Ohm). Vorsicht Verwenden Sie nur die Antennen aus dem Zubehörsortiment von SINAUT Telecontrol, die für das MD740-1 bestimmt sind. Andere Antennen können die Geräteeigenschaften negativ beeinflussen und sogar zu Defekten führen.
4	Service Schnittstelle: Optional: Zum Anschließen eines PCs zur Anzeige von Geräte-, Status- und Verbindungsinformationen. Zum Anschließen eines V.24-Kabels.
5	Applikations-Schnittstelle. Schließen Sie hier das Gerät mit Ethernet-Schnittstelle an, das über das GPRS kommunizieren soll. Bei Anschluss an die Netzwerkkarte eines Rechners benutzen Sie ein Cross-Over Ethernet Kabel. Bei Anschluss ans Netzwerk benutzen Sie ein Patch-Ethernet-Kabel.

Tabelle 3-3 Anschlüsse des MD740-1

Ein- und Ausschalten

Das MD740-1 wird eingeschaltet, indem es an die Stromversorgungsquelle angeschlossen wird (siehe Kap. 3.1).

Nach dem Einschalten leuchtet zuerst die LED *DC5V*. Sofern das Gerät gültig konfiguriert und die SIM-Karte eingesteckt ist, bucht sich das Gerät automatisch ins GPRS-Netz ein. Sobald die LED *C (Connect)* leuchtet, besteht eine GPRS-Verbindung. Das Gerät ist so konzipiert, dass es ständig eingeschaltet sein kann.

Ausschalten erfolgt durch Trennen von der Stromversorgung.

3.2 PIN konfigurieren

Damit das MD740-1 über das GPRS-Netz Ihres Netzbetreibers kommunizieren kann, müssen Sie dem Gerät die PIN (Persönliche Identifikations-Nummer) der SIM-Karte bekannt geben. Erst danach setzen Sie die SIM-Karte in das Gerät ein.

Hat Ihre SIM-Karte keine PIN, tragen Sie trotzdem eine beliebige PIN ein, z. B. 0000.

Zur Konfiguration der PIN gehen Sie bitte wie folgt vor:

1. Mit Ihrem Web-Browser (z. B. MS Internet Explorer) stellen Sie eine Konfigurations-Verbindung zum MD740-1 her. Folgen Sie dabei der Beschreibung im Kapitel 4.1.

2. Sobald die Administrator-Website des MD740-1 angezeigt wird, wählen Sie Netzwerk → GPRS.

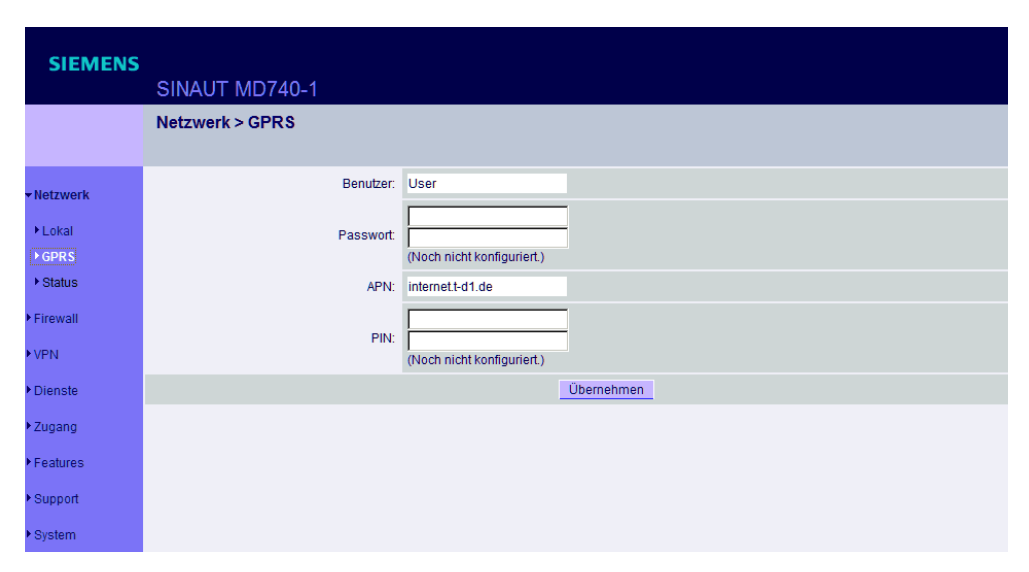


Abbildung 3-2

3. In die Eingabefelder PIN geben Sie die PIN der SIM-Karte ein, die Sie anschließend ins Gerät einsetzen werden. Geben Sie die PIN übereinstimmend in beide Felder ein.

4. Klicken Sie dann *Übernehmen*.

5. Ist eine PIN gesetzt, wird die Meldung „Noch nicht konfiguriert." nicht mehr angezeigt.

6. Sie können die Verbindung wieder trennen, indem Sie den Web-Browser schließen.

3.3 SIM-Karte einlegen oder wechseln

Achtung

Stellen Sie sicher, dass das Gerät von der Versorgungsspannung getrennt ist.

Um die SIM-Karte einzulegen, müssen Sie das Gehäuse des MD740-1 öffnen.

Auf dem Gehäuse befinden sich auf der Oberseite und auf der Unterseite jeweils zwei Verschlüsse mit Öffnungsklemmen.



Abbildung 3-3

1. Entriegeln Sie die beiden Öffnungsklemmen des Gehäuseteils mit Antennenanschluss. Dazu drücken Sie die zugehörigen Öffnungsklemmen mit einem geeigneten Gegenstand vorsichtig an (siehe Bild unten), so dass sich der Verschluss öffnet.



Abbildung 3-4

2. An dem entriegelten Teil etwas ziehen, so dass sich das Gehäuse öffnet.

Achtung

Die Platinen in den beiden vorderen Gehäuseteile sind durch ein IO-Kabel miteinander verbunden. Achten Sie beim Herausziehen darauf, diese Kabelverbindung nicht zu lösen oder zu beschädigen. Entriegeln Sie gegebenenfalls beide vorderen Gehäuseteile und ziehen Sie sie vorsichtig zusammen heraus



Abbildung 3-5

Auf der Platine ist der Halter der SIM-Karte sichtbar.

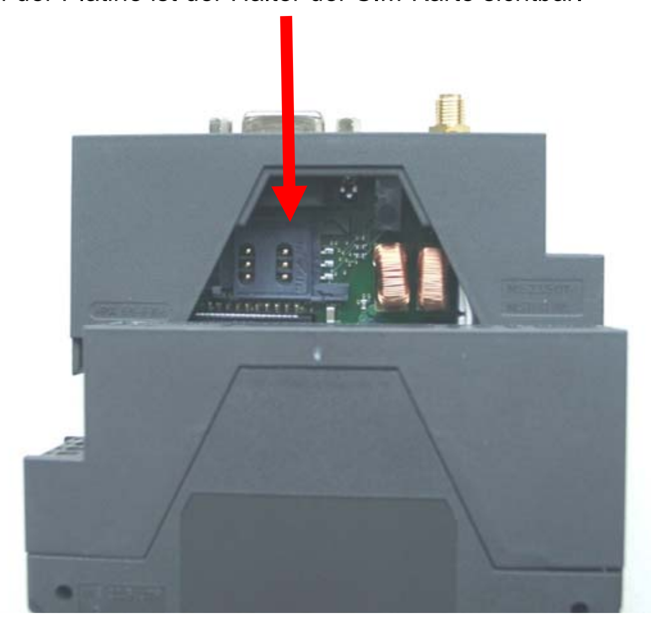


Abbildung 3-6

3. Mit dem Fingernagel oder einem geeigneten Gegenstand das Oberteil des SIM-Karten-Halters ungefähr 2 mm in Pfeilrichtung nach links schieben (siehe weißer Pfeil in der Abbildung), damit sich das Oberteil hochklappen lässt.



Abbildung 3-7

4. Das Oberteil des SIM-Karten-Halters hochklappen, damit Sie die SIM-Karte in dieses Teil einschieben können. In der Abbildung 3-8 ist das Fach, in das Sie die SIM-Karte einschieben können, weiß hervorgehoben.

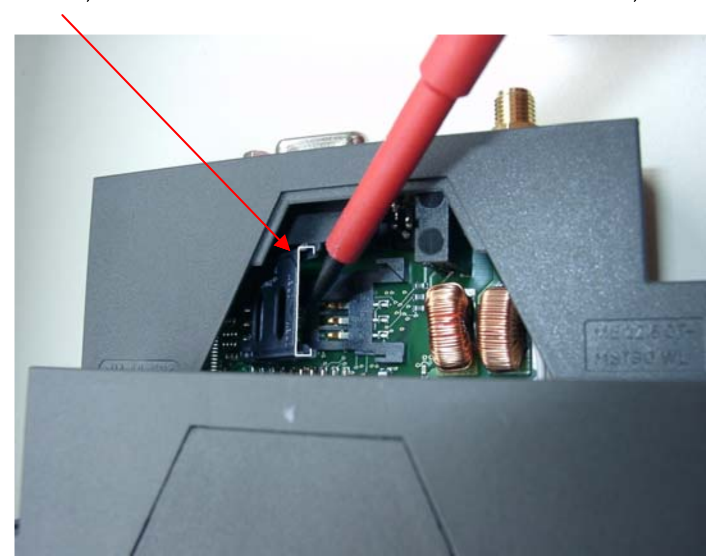


Abbildung 3-8

5. Die SIM-Karte so in das Oberteil des SIM-Karten-Halters einschieben, dass die Kontaktfläche unten liegt und die abgeschrägte Ecke der SIM-Karte zur Vorderseite des Gerätes zeigt (siehe Abbildung 3-9 und Abbildung 3-10).

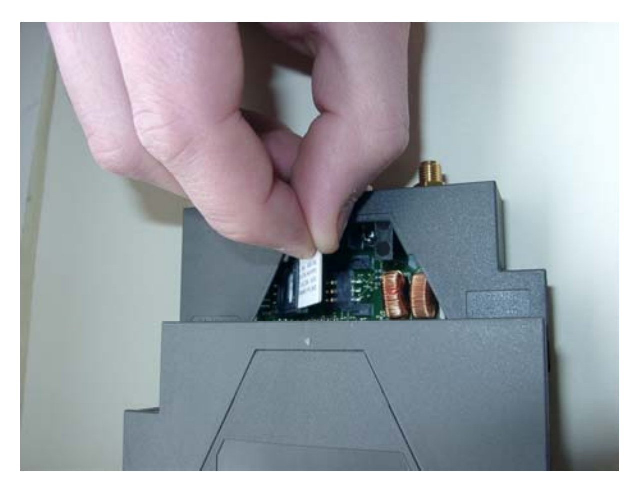


Abbildung 3-9

6. Die SIM-Karte so weit einschieben, dass das Oberteil des SIM-Karten-Halters wieder nach unten geklappt werden kann.



Abbildung 3-10

7. Das Oberteil des SIM-Karten-Halters nach unten drücken. Achten Sie auf den Sitz der abgeschrägten Ecke der SIM-Karte (siehe Abbildung 3-11).



Abbildung 3-11

8. Mit dem Fingernagel oder einem geeigneten Gegenstand das Oberteil des SIM-Karten-Halters ungefähr 2 mm in Pfeilrichtung nach rechts schieben (siehe roter Pfeil in Abbildung 3-12), um den SIM-Karten-Halter zu verriegeln.

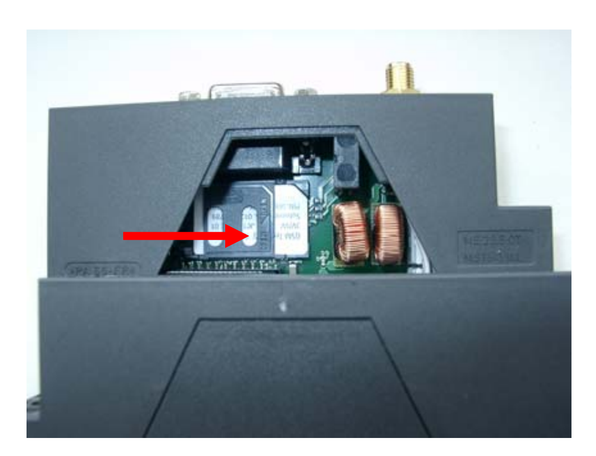


Abbildung 3-12

Nach Abschluss der Operation ist die SIM-Karte fest im SIM-Karten-Halter verriegelt.

9. Kontrollieren Sie die Verbindung des internen IO-Kabels.

10. Abschließend die Gehäuseteile wieder zusammenschieben und aneinander drücken, damit die Klemmen der Verschlüsse oben und unten einrasten.

Konfiguration

4

4.1 Übersicht

Die Konfiguration der Router-, VPN- und Firewall-Funktionen erfolgt lokal oder aus der Ferne über die Web-Site des Router-Teils.

Fernkonfiguration

Eine Fernkonfiguration, also die Konfiguration von einem entfernten Ort aus, ist nur möglich, sofern das MD740-1 für Fernzugriff konfiguriert ist. Sie gehen in diesem Fall genauso vor, wie in Abschnitt *Konfigurations-Verbindung herstellen* beschrieben.

Lokale Konfiguration

Voraussetzungen für eine lokale Konfiguration sind:

- Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  - direkt an der Ethernet-Buchse des MD740-1 per Cross-Over-Netzwerkkabel angeschlossen sein

    oder

  - er muss per LAN direkten Zugriff auf das MD740-1 haben.
- Der Netzwerkadapter des Rechners, mit dem Sie die Konfiguration vornehmen, muss folgende TCP/IP Konfiguration haben:

  IP-Adresse: **192.168.1.2**

  Subnetzmaske: **255.255.255.0**
  Standardgateway: **192.168.1.1**
  Bevorzugter DNS-Server: **Adresse des Domain Name Servers**

TCP/IP Konfiguration des Netzwerkadapters unter Windows XP oder Windows 2000

1. Klicken Sie *Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen*

   Symbol des LAN-Adapters mit der rechten Maustaste klicken und im Kontextmenü *Eigenschaften* klicken.

   Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter *Diese Verbindung verwendet folgende Elemente* den Eintrag *Internetprotokoll (TCP/IP)* markieren und dann die Schaltfläche *Eigenschaften* klicken.

   Es erscheint das Fenster *Eigenschaften von Internetprotokoll TCP/IP* (siehe Abbildung unten).

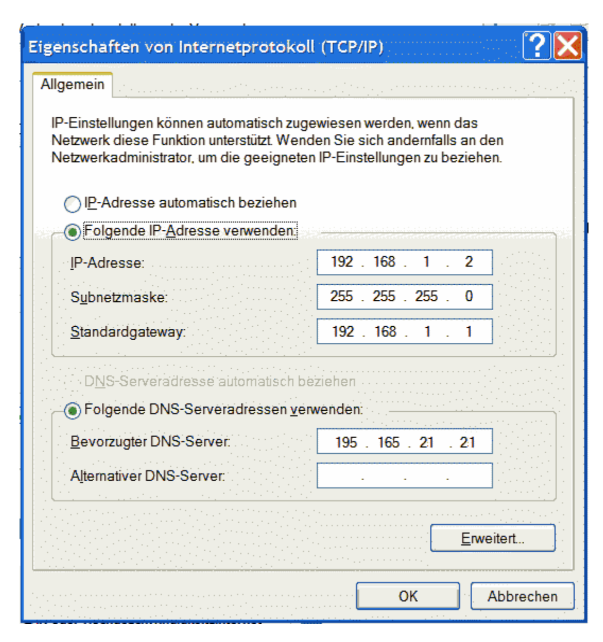


Abbildung 4-1

2. Geben Sie folgende Werte ein:

   IP-Adresse: **192.168.1.2**
   Subnetzmaske: **255.255.255.0**
   Standardgateway: **192.168.1.1**
   Bevorzugter DNS-Server: **Adresse des Domain Name Servers**

Bevorzugter DNS-Server

Wenn Sie Adressen über einen Domain-Namen aufrufen (z. B. www.siemens.de), dann muss auf einem Domain Name Server (DNS) nachgeschlagen werden, welche IP-Adresse sich hinter dem Namen verbirgt. Als Domain Name Server können Sie festlegen:

- DNS-Adresse des Netzbetreibers

  oder

- Lokale IP-Adresse des MD740-1, sofern dieses zum Auflösen von Hostnamen in IP-Adressen konfiguriert ist (siehe Kapitel 4.5).

Um den Domain Name Server in der TCP/IP-Konfiguration Ihres Netzwerkadapters festzulegen, gehen Sie wie oben beschrieben vor.

Konfigurations-Verbindung herstellen

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.

   (Z. B. MS Internet Explorer ab Version 5.0 oder Netscape Communicator ab Version 4.0; der Web-Browser muss SSL (d. h. https) unterstützen.)

2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt.

   Im MS Internet Explorer nehmen Sie diese Einstellung wie folgt vor: Menü *Extras, Internetoptionen...*, Registerkarte *Verbindungen*: Unter *DFÜ- und VPN-Einstellungen* muss *Keine Verbindung wählen* aktiviert sein.

3. In der Adresszeile des Browsers geben Sie die Adresse des MD740-1 vollständig ein. Gemäß Werkseinstellung lautet diese:

   https://192.168.1.1

   Folge: Der auf der nächsten Seite abgebildete Sicherheitshinweis erscheint.

Falls die Administrator-Website nicht angezeigt wird

Sollte auch nach wiederholtem Versuch der Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Überprüfen Sie die Hardware-Verbindung.
  Dazu bei einem Windows-Rechner über die DOS-Eingabeaufforderung (Menü *Start, Programme, Zubehör, Eingabeaufforderung*) folgenden Befehl eingeben:

  ping 192.168.1.1

  Wenn innerhalb der vorgegebenen Zeitspanne die Meldung über den Rück-Empfang der 4 ausgesendeten Pakete nicht erscheint, überprüfen Sie bitte das Kabel, die Anschlüsse und die Netzwerkkarte.

- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet.

Im MS Internet Explorer (Version 6.0) nehmen Sie diese Einstellung wie folgt vor: Menü *Extras, Internetoptionen...*, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche *Einstellungen...* klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter *Proxyserver* der Eintrag *Proxyserver für LAN verwenden* nicht aktiviert ist.

- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü *Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen* bzw. *Netzwerk- und DFÜ-Verbindungen* das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü *Deaktivieren* wählen.

- Geben Sie die Adresse des MD740-1 mit Slash ein:

  https://192.168.1.1/

Bei erfolgreichem Aufbau der Verbindung

Nach erfolgreicher Verbindungsaufnahme erscheint dieser Sicherheitshinweis:

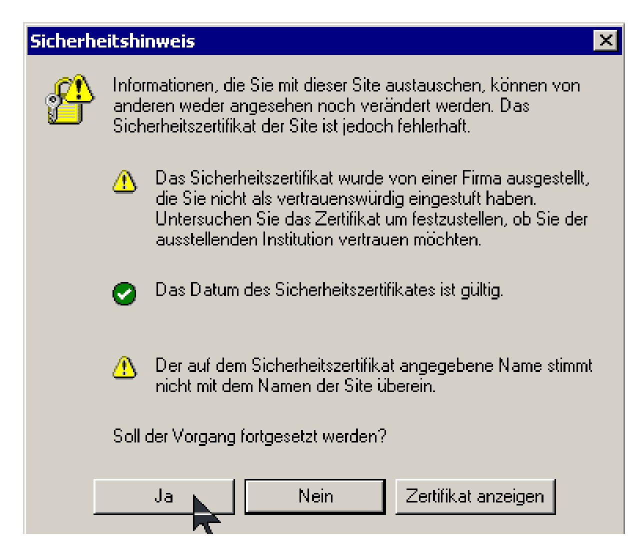


Abbildung 4-2

4. Quittieren Sie den entsprechenden Sicherheitshinweis mit Ja

---

Hinweis

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erfolgt ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen. Aus dem Zertifikat muss erkenntlich sein, dass es für das SINAUT MD740-1 ausgestellt wurde. Die Administrator-Website wird über eine IP-Adresse adressiert und nicht über einen Namen, daher stimmt der im Sicherheitszertifikat angegebene Name nicht mit dem im Zertifikat überein.

---

5. Sie werden aufgefordert, den Benutzernamen und das Passwort anzugeben:



Abbildung 4-3

Die werksseitige Voreinstellung lautet:

Benutzername: **admin**
Passwort: **sinaut**

Startseite der Administrator-Webseite

6. Folge: Die Administrator-Website des MD740-1 wird angezeigt.



Abbildung 4-4

Zur Konfiguration gehen Sie wie folgt vor:

1. Per Menü den gewünschten Einstellbereich aufrufen.
2. Auf der betreffenden Seite die gewünschten Einträge machen.

3. Mit *Übernehmen* ggf. bestätigen, so dass die Einstellungen vom Gerät übernommen werden.

   Sollte bei erneuter Anzeige einer Seite diese nicht aktuell sein, weil der Browser sie aus dem Cache lädt, aktualisieren Sie die Anzeige der Seite. Dazu in der Browser-Symbolleiste das Symbol zum Aktualisieren klicken.

Hinweis

Je nachdem, wie Sie das MD740-1 konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

Tragen Sie bei der Eingabe von IP-Adressen, die IP-Adress-Teilnummern immer ohne führende Nullen ein, z.B.: 192.168.0.8.

4.2 Menü Netzwerk

4.2.1 Netzwerk → Lokal

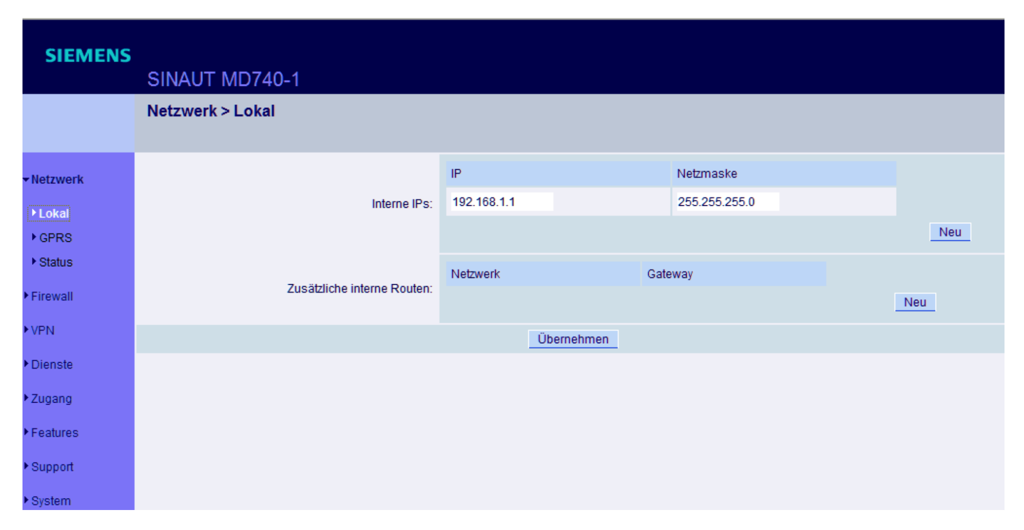


Abbildung 4-5

Interne IPs

Eine interne IP ist die IP-Adresse, unter der das MD740-1 von Geräten des lokal angeschlossenen Netzes erreichbar ist.

Die IP-Adresse ist werksseitig wie folgt voreingestellt:

IP-Adresse:	**192.168.1.1**
Lokale Netzmaske:	**255.255.255.0**

Sie können weitere Adressen festlegen, unter denen das MD740-1 von Geräten des lokal angeschlossenen Netzes angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das lokal angeschlossene Netz in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen das MD740-1 unter unterschiedlichen Adressen erreichen.

Weitere interne IP festlegen

Wollen Sie eine weitere interne IP festlegen, klicken Sie *Neu*. Sie können beliebig viele interne IPs festlegen.

Interne IP löschen

Wollen Sie eine interne IP löschen, klicken Sie *Löschen*. (Die erste IP-Adresse in der Liste können Sie nicht löschen.)

Zusätzliche interne Routen

Sind am lokal angeschlossen Netz weitere Subnetze angeschlossen, können Sie zusätzliche Routen definieren.

Siehe auch Kapitel 4.11.

Wollen Sie eine weitere Route zu einem Subnetz festlegen, klicken Sie *Neu*.

Geben Sie an:

- die IP-Adresse des Subnetzes (Netzwerkes), ferner

- die IP-Adresse des Gateways, über das das Subnetz angeschlossen ist.

Sie können beliebig viele interne Routen festlegen.

Wollen Sie eine interne Route löschen, klicken Sie *Löschen*.

4.2.2 Netzwerk → GPRS

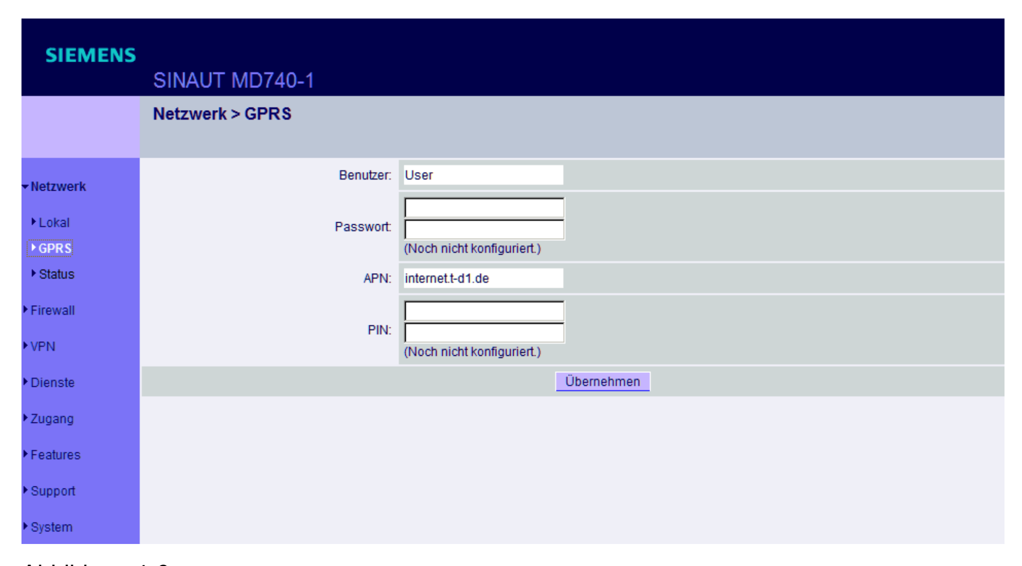


Abbildung 4-6

Benutzer (Benutzername):

Name des Benutzers.

Passwort

Wenn sich das MD740-1 im GPRS-Netz anmeldet, werden im Allgemeinen Benutzername und Passwort von ihm abgefragt, damit es Zugang zum Netz erhält.

Einige GSM/GPRS-Netzbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld ein: **gast**

Hinweise

- Ihren Benutzernamen und Ihr Passwort finden Sie in den Unterlagen von Ihrem Netzbetreiber.
- Tragen Sie das Passwort übereinstimmend in beide Felder ein.

Ist ein Passwort gesetzt, wird die Meldung „Noch nicht konfiguriert." nicht mehr angezeigt.

APN (Access Point Name = Zugriffspunktname)

Bezeichnet den Netz-Übergang

- zum Internet. In diesem Fall ist die Gegenstelle über das Internet erreichbar.
  oder
- zum privaten Netzwerk. In diesem Fall ist die Gegenstelle über eine gemietete Standleitung mit dem GPRS-Netzbetreiber verbunden.

Hinweise

- Bei Internet-APN:

  Sie finden den APN in den Unterlagen Ihres GSM/GPRS-Netzbetreibers, auf seiner Internetseite oder erfragen ihn bei dessen Hotline.
- Bei privatem APN:

  Sie erhalten die Zugangsdaten bei Ihrem Netzbetreiber.

PIN der im Gerät eingesetzten SIM-Karte

Damit das MD740-1 mit der SIM-Karte des Netzbetreibers arbeiten kann, muss dem Gerät die PIN (Persönliche Identifikations-Nummer) der SIM-Karte bekannt gegeben werden - sofern die SIM-Karte eine PIN hat. Erst danach setzen Sie die SIM-Karte in das *ausgeschaltete* Gerät ein.

Geben Sie dazu die PIN ein und klicken Sie *Übernehmen*.

Ist eine PIN gesetzt, wird die Meldung „Noch nicht konfiguriert." nicht mehr angezeigt.

Hinweise

- Die PIN übereinstimmend in beide Felder eintragen.
- Die eingegebene PIN muss mit der PIN der SIM-Karte übereinstimmen, mit der das Gerät arbeiten soll.
- Sie können mit diesem Gerät nicht die PIN der SIM-Karte ändern.

4.2.3 Netzwerk → Status



Abbildung 4-7

Folgende Statusangaben werden angezeigt:

Netzwerk-Modus

Gibt an, ob eine GPRS-Verbindung besteht (Anzeige: "modem up") oder im Wartezustand ist (Anzeige: „(none)“ oder "modem (later)").

Externe IP:

Die IP-Adresse, unter der das Gerät von außen erreichbar ist. Diese IP-Adresse wird dem Gerät vom Betreiber des GPRS-Netzes für die jeweils aktuelle Verbindung zugewiesen.

Default Gateway über externe IP:

IP-Adresse des integrierten GPRS-Modems. Dieses Gateway wirkt vom VPN-Router zum externen Netz (z. B. Internet).

4.3 Menü Firewall

Das MD740-1 beinhaltet eine *Stateful Packet Inspection Firewall*.

Eingehende Verbindung:

Die Regeln für eintreffende Daten sind zu definieren, die Regeln für abgehende Daten dieser Verbindung ergeben sich automatisch aus den Regeln für die eintreffenden Daten; bei Umkonfiguration der Verbindung werden noch ausstehende Daten weiterhin entsprechend den alten Regeln ausgesendet.

Abgehende Verbindung:

Die Regeln für abgehende Daten sind zu definieren, die Regeln für eintreffende Daten dieser Verbindung ergeben sich automatisch aus den Regeln für die abgehenden Daten; bei Umkonfiguration der Verbindung werden noch ausstehende Daten weiterhin entsprechend den alten Regeln empfangen.

Werksseitige Voreinstellung der Firewall

Alle eingehenden Verbindungen werden abgewiesen (außer VPN).

Die Datenpakete aller ausgehenden Verbindungen werden abgewiesen (außer VPN und außer Verbindungen zur integrierten Webseite, die über Geräte- und Verbindungsdaten informiert).

Hinweise

- VPN-Verbindungen unterliegen nicht den unter diesem Menüpunkt festgelegten Firewall-Regeln. Firewall-Regeln für jede einzelne VPN-Verbindung können Sie unter Menü VPN → Verbindungen festlegen.
- Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

4.3.1 Firewall → Eingehend

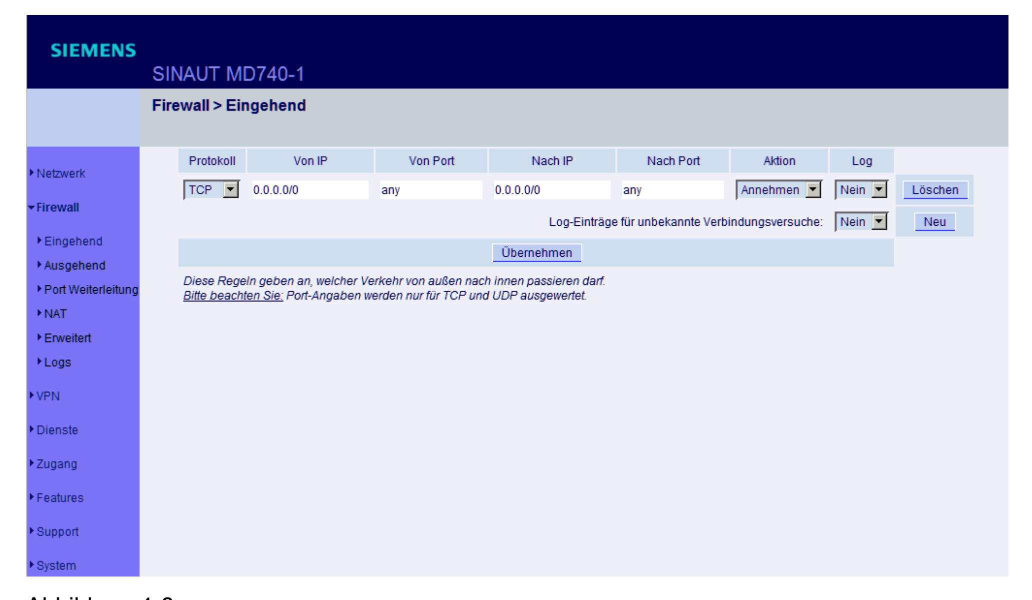


Abbildung 4-8

Das Fenster ‘Firewall eingehend’ listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.

- Ist keine Regel gesetzt, werden alle eingehenden Verbindungen (außer VPN) abgewiesen (= Werkseinstellung).

Regel löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*. Dann *Übernehmen*.

Regel neu setzen

Wollen Sie eine neue Regel setzen, klicken Sie *Neu*. Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie *Übernehmen*.

Zur Bestätigung erhalten Sie eine Systemmeldung.

Angaben beim Löschen und Neusetzen von Regeln

Protokoll:

Alle bedeutet: TCP, UDP, ICMP und andere.

Von / nach IP:

Angabe der IP-Adresse bzw. -Adressenbereichs. ***0.0.0.0/0*** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 4.10.

Von / nach Port:
(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

*startport***:**endport (z. B. 110**:**120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Portnummer oder mit dem entsprechenden Servicenamen angeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion:

Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.

Log:

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

– das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen

– oder nicht - *Log* auf *Nein* setzen (werksseitige Voreinstellung)

Log-Einträge für unbekannte Verbindungsversuche:

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

4.3.2 Firewall → Ausgehend

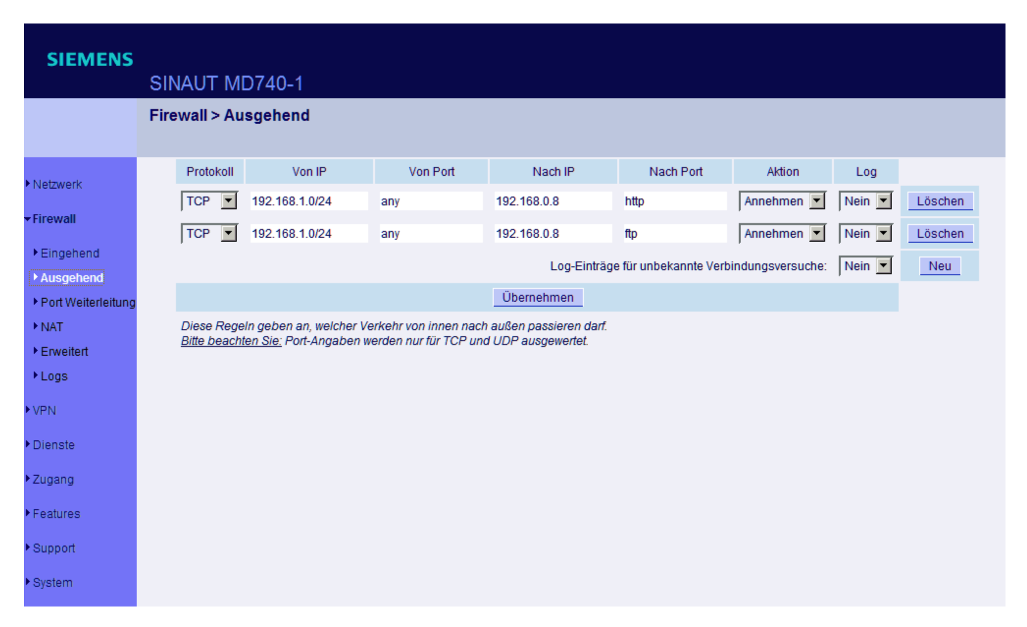


Abbildung 4-9

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenpakete, die zu GPRS-Verbindungen gehören, die das MD740-1 initiiert, um mit einer entfernten Gegenstelle zu kommunizieren.

Hinweis

- Ist keine Regel gesetzt, sind alle ausgehenden Verbindungen verboten (außer VPN).
- Werkseinstellung: Ausgehende Verbindungen verboten (außer VPN und Verbindungen zur integrierten Webseite, die über Geräte- und Verbindungsdaten informiert).

Regel löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*. Dann *Übernehmen*.

Neue Regel setzen

Wollen Sie eine neue Regel setzen, klicken Sie *Neu.* Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie *Übernehmen*.

Zur Bestätigung erhalten Sie eine Systemmeldung.

Angaben beim Löschen und Neusetzen von Regeln

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll:

Alle bedeutet: TCP, UDP, ICMP und andere.

Von / nach IP:

IP-Adresse oder -Adressenbereich. ***0.0.0.0/0*** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise – siehe Kapitel 4.10.

Von / nach Port:
(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Portnummer oder mit dem entsprechenden Servicenamen angeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion:

Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Log:

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

– das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen

– oder nicht - *Log* auf *Nein* setzen (werksseitige Voreinstellung)

Log-Einträge für unbekannte Verbindungsversuche:

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

4.3.3 Firewall → Port Weiterleitung



Abbildung 4-10

Listet die festgelegten Regeln zur Port Weiterleitung auf.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse des MD740-1 sowie an einen bestimmten Port des MD740-1 gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden.
D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT oder Port Forwarding genannt.

Hinweis

Die hier eingestellten Regeln haben Vorrang gegenüber den Einstellungen unter *Firewall → Eingehend*.

Regel löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*, dann *Übernehmen*.

Neue Regel setzen

Wollen Sie eine neue Regel setzen, klicken Sie *Neu*. Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie *Übernehmen*.

Angaben beim Löschen und Neusetzen von Regeln

Protokoll

Geben Sie hier das Protokoll an, auf das sich die Regel beziehen soll.

Eintreffend auf IP

Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des MD740-1 an.

ODER

Falls ein dynamischer Wechsel der externen IP-Adresse des MD740-1 erfolgt, so dass diese nicht angebbar ist, verwenden Sie folgende Variable: **%extern**.

Die Angabe von **%extern** bezieht sich bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface immer auf die erste IP-Adresse der Liste.

Eintreffend auf Port

Original-Ziel-Port, der in eingehenden Datenpaketen angegeben ist.

Weiterleiten an IP

Interne IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben werden.

Weiterleiten an Port

Port, an den die Datenpakete weitergeleitet werden sollen und auf den die Original-Port-Angaben umgeschrieben werden.

Bei den Angaben haben Sie folgende Möglichkeiten:

Port

Sie können nur einzelne Ports angeben, entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen: (z. B. 110 für pop3 oder pop3 für 110).

Log

Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
- oder nicht - *Log* auf *Nein* setzen (Werkseinstellung).

4.3.4 Firewall → NAT

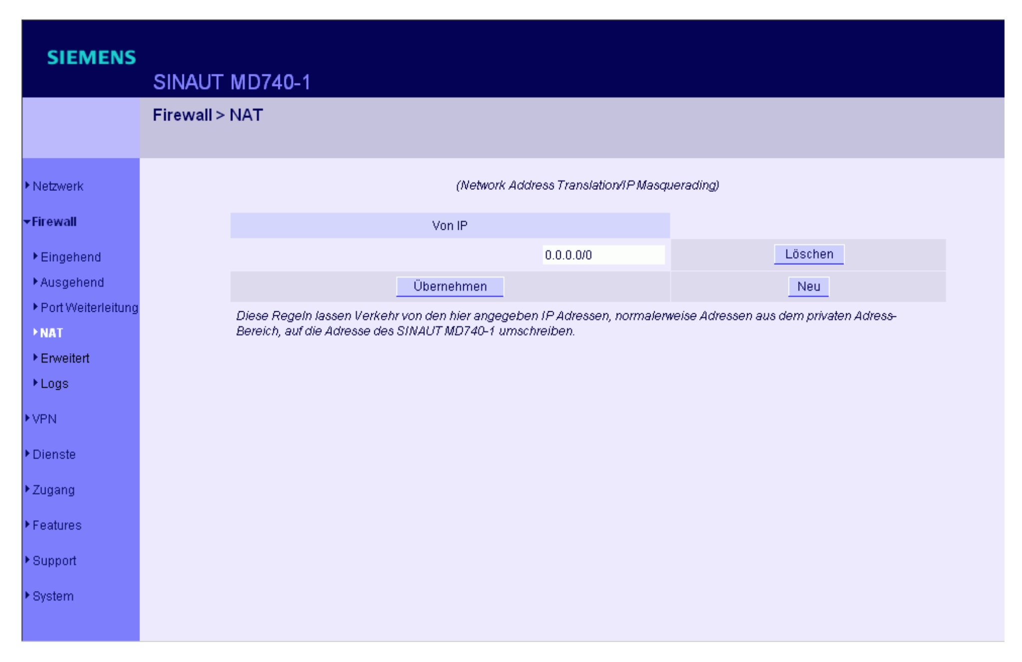


Abbildung 4-11

Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf und ermöglicht, Regeln zu setzen oder zu löschen.

Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x benutzt wird oder weil die interne Netzstruktur verborgen werden soll.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

Werkseinstellung: Es findet NAT statt.

Regel löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*, dann *Übernehmen***.**

Neue Regel setzen

Wollen Sie eine neue Regel setzen, klicken Sie *Neu*.
Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie *Übernehmen*.

Angaben beim Löschen und Neusetzen von Regeln

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

0.0.0.0/0 bedeutet alle Adressen, d. h. alle internen IP-Adressen werden dem NAT-Verfahren unterzogen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 4.10.

4.3.5 Firewall → Erweiterte Einstellungen

Diese Einstellungen bestimmen das grundlegende Verhalten der Firewall.

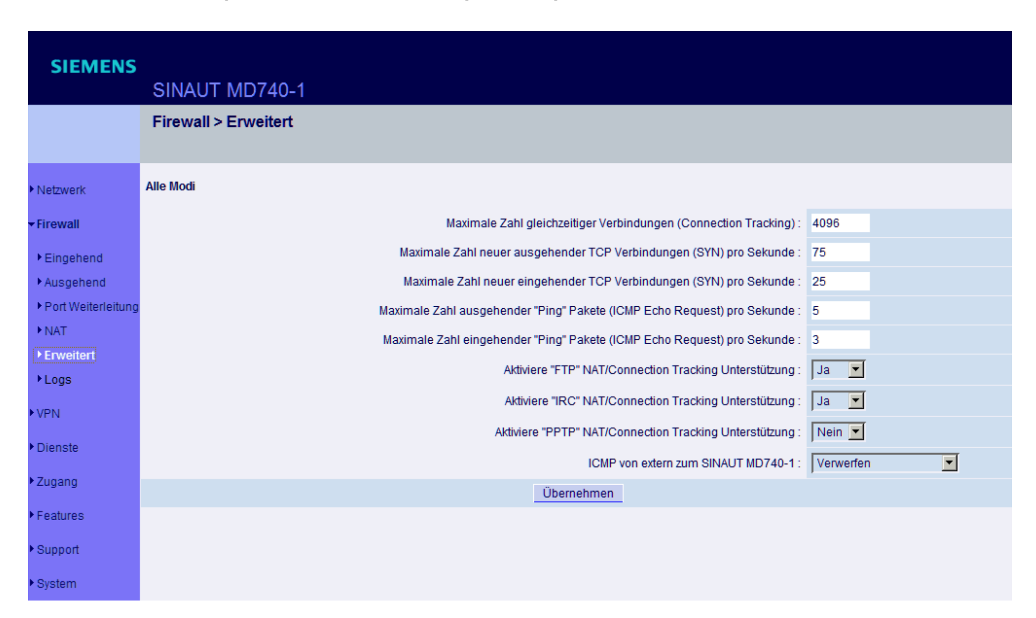


Abbildung 4-12 Standardwerte der erweiterten Einstellungen der Firewall

Maximale Zahl ...
Die ersten 5 Einträge legen Obergrenzen fest. Die Voreinstellungen (siehe Abbildung) sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Aktiviere „FTP“ NAT/Connection Tracking Unterstützung
Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss **Aktiviere „FTP“ NAT/Connection Tracking Unterstützung** auf *Ja* stehen (Standard).

Aktiviere „IRC“ NAT/Connection Tracking Unterstützung
Ähnlich wie bei FTP: Beim Chatten im Internet per IRC müssen nach aktivem Verbindungsaufbau auch eingehende Verbindungen zugelassen werden, soll das Chatten reibungslos funktionieren. Damit diese von der Firewall durchgelassen werden, muss **Aktiviere „IRC“ NAT/Connection Tracking Unterstützung** auf *Ja* stehen (Standard).

Aktiviere „PPTP“ NAT/Connection Tracking Unterstützung
Muss nur dann auf *Ja* gesetzt werden, wenn folgende Bedingung vorliegt:

Von einem lokalen Rechner soll ohne Zuhilfenahme des MD740-1 eine VPN-Verbindung mittels PPTP zu einem externen Rechner aufgebaut werden. Werksseitig ist dieser Schalter auf *Nein* gesetzt.

ICMP von extern zum MD740-1
Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz an das MD740-1 gesendet werden. Sie haben folgende Möglichkeiten:

- **Verwerfen**: Alle ICMP-Nachrichten zum MD740-1 werden verworfen.
- **Annehmen von Ping**: Nur Ping-Nachrichten (ICMP Typ 8) zum MD740-1 werden akzeptiert.
- **Alle ICMPs annehmen**: Alle Typen von ICMP Nachrichten zum MD740-1 werden akzeptiert.

4.3.6 Firewall → Logs

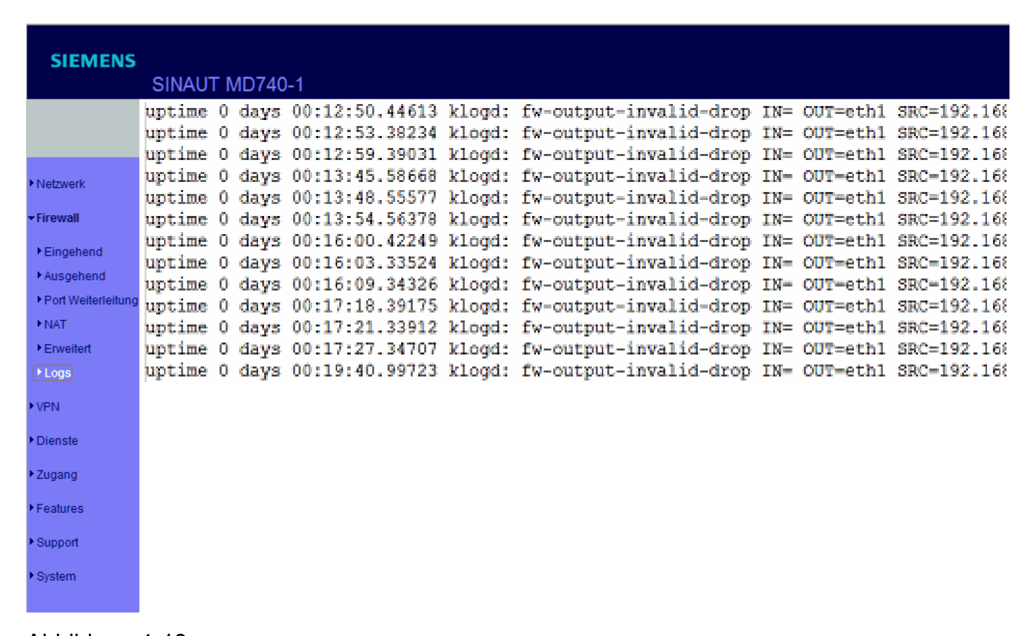


Abbildung 4-13

Nur Anzeige:

Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = Ja), dann können Sie hier das Log aller protokollierten Ereignisse einsehen.

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

4.4 Menü VPN

Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Partner bekannt und zugänglich sind. Siehe Kapitel 1.3.

Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:

- Authentifizierung über Pre-Shared Key (PSK) oder X.509 Zertifikate
- ESP
- Diffie-Hellman Gruppe 2 oder 5
- DES, 3DES oder AES encryption
- MD5 oder SHA-1 Hash Algorithmen
- Tunnel oder Transport Modus
- Quick Mode
- Main Mode
- SA Lifetime (1 Sekunde bis 24 Stunden)

Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.

Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough). In beiden Fällen sind aus technischen Gründen nur IPsec Tunnel-Verbindungen möglich.

4.4.1 VPN-Verbindungen



Abbildung 4-14

Listet die eingerichteten VPN-Verbindungen auf. Sie können jede einzelne Verbindung aktivieren (Aktiv = *Ja*) oder deaktivieren (Aktiv = *Nein*).

VPN-Verbindung löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*.
Klicken Sie abschließend *Übernehmen*.

Neue VPN-Verbindung einrichten

Klicken Sie *Neu*.
Geben Sie der Verbindung einen Namen und klicken Sie *Editieren*.
Machen Sie die gewünschten bzw. erforderlichen Einstellungen (s. u.).
Klicken Sie abschließend *Übernehmen*.

VPN-Verbindung bearbeiten

Klicken Sie neben der betreffenden Verbindung die Schaltfläche *Editieren*.
Machen Sie die gewünschten bzw. erforderlichen Einstellungen (siehe nachfolgende Abbildung und Erläuterungen).
Klicken Sie abschließend *Übernehmen*.

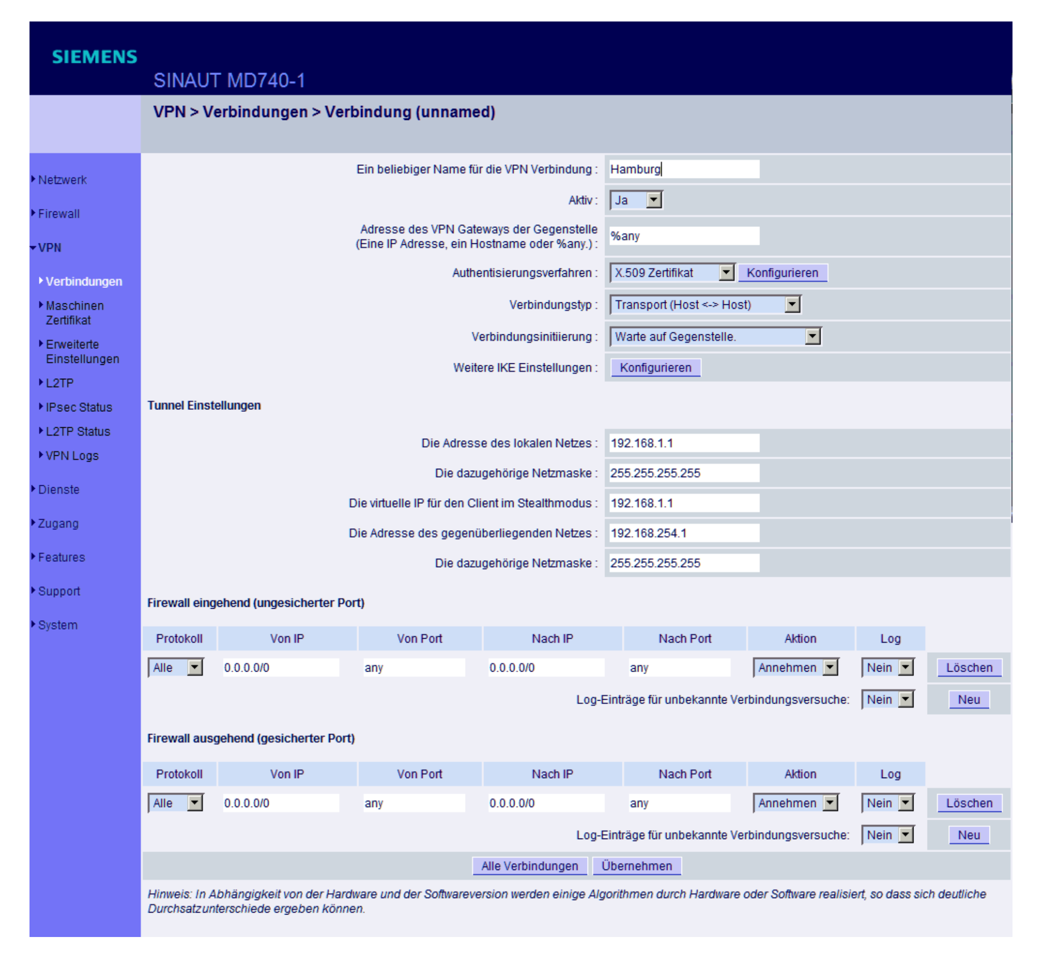


Abbildung 4-15

Ein beliebiger Name für die VPN Verbindung

Sie können die Verbindung frei benennen bzw. umbenennen.

Aktiv

Legen Sie fest, ob die Verbindung aktiv (= *Ja*) sein soll oder nicht (= *Nein*).

Adresse des VPN Gateways der Gegenstelle

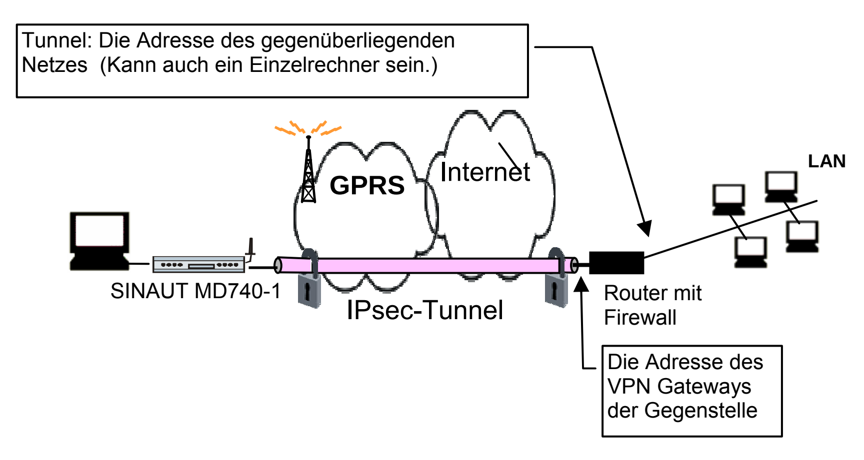


Abbildung 4-16

Gemeint ist die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet - siehe Abbildung oben.

Falls das MD740-1 aktiv die Verbindung zur entfernten Gegenstelle initiieren und aufbauen soll, dann geben Sie hier die IP-Adresse der Gegenstelle an. Statt einer IP-Adresse können Sie auch einen Hostnamen (d. h. Domain Namen im URL-Format in der Form www.xyz.de) eingeben.
Falls der VPN Gateway der Gegenstelle keine feste und bekannte IP-Adresse hat, kann über die Inanspruchnahme des DynDNS-Service dennoch eine feste und bekannte Adresse simuliert werden. Siehe Kapitel 1.3.

Falls das MD740-1 bereit sein soll, die Verbindung anzunehmen, die eine entfernte Gegenstelle mit beliebiger IP-Adresse aktiv zum lokalen MD740-1 initiiert und aufbaut, dann geben Sie an: **%any**
Dann kann eine entfernte Gegenstelle, die ihre eigene IP-Adresse (vom Internet Service Provider) dynamisch zugewiesen erhält, d. h. eine wechselnde IP-Adresse hat, das lokale MD740-1 „anrufen".
Baut ausschließlich eine bestimmte Gegenstelle mit fester IP-Adresse die Verbindung auf, können Sie sicherheitshalber deren IP-Adresse angeben.

Hinweis

Damit eine Verbindung zum MD740-1 aufgebaut werden kann, benötigt das MD740-1 eine feste IP-Adresse, durch den Provider oder durch Nutzung eines DynDNS-Service.

Hinweis

Der Verbindungsaufbau von einer entfernten Gegenstelle zum MD740-1 wird in vielen GSM/GPRS-Netzen nicht unterstützt.

Authentisierungsverfahren

Es gibt 2 Möglichkeiten:

- X.509 Zertifikat
- Pre-Shared Key

X.509 Zertifikat

Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. Dabei verschlüsselt das MD740-1 die Authentifizierungs-Datagramme, die es zur Gegenstelle, dem „Tunnelende", sendet, mit dem öffentlichen Schlüssel (Dateiname *.cer oder *.pem) der Gegenstelle. (Diese *.cer- oder *.pem-Datei haben Sie vom Bediener der Gegenstelle erhalten, z. B. per Diskette oder per E-Mail).

Um diesen öffentlichen Schlüssel dem MD740-1 zur Verfügung zu stellen, gehen Sie wie folgt vor:

Voraussetzung:

Sie haben die *.cer- oder *.pem-Datei auf dem lokal angeschlossenen Rechner gespeichert.

1. *Konfigurieren* klicken.

   Folge: Der Bildschirm VPN > Verbindungen > Verbindung xyz > X.509 Zertifikat erscheint. („xyz" ist der jeweilige Name der Verbindung.)

2. *Durchsuchen...* klicken und die Datei selektieren.

3. *Import* klicken.

   Nach dem Import wird der Inhalt des neuen Zertifikats angezeigt - siehe nachfolgende Abbildung. Eine Erläuterung der angezeigten Informationen finden Sie im Kapitel 4.4.2.



Abbildung 4-17

Lokale ID und Remote ID

Die Lokale ID und die Remote ID werden vom IPsec (freeswan) genutzt, um beim Aufbau eines Tunnels die eindeutige Identifikation des Tunnels, und somit der Tunnelkonfiguration, zu ermitteln. Normalerweise entsprechen die Identifier bei Nutzung von X.509 den Distinguished Names der Zertifikate, denn diese sind immer eindeutig, sofern in der Konfiguration angegeben. Wenn jedoch %any verwendet wird, kann der Distinguished Name der Gegenstelle nicht unbedingt eindeutig einer Tunnelkonfiguration zugeordnet werden, und u.U. wird eine falsche benutzt, was dann zum Fehlschlagen des Aufbaus der Verbindung führen kann.

Hier kann mittels Remote ID und Lokale ID dann Abhilfe geschaffen werden:

- das, was bei der Gegenstelle als Lokale ID genutzt wird, wird beim MD740-1 als Remote ID eingestellt,
- und das, was die Gegenstelle als Identifier erwartet, um die Verbindung von MD740-1 zu identifizieren, wird beim MD740-1 als Lokale ID eingetragen.

Es kann gut sein, dass die Lokale ID in Ihrem Einsatzfall nicht konfiguriert werden muss, weil z.B. die Gegenstelle nur eine Verbindung konfiguriert hat, und somit eine Identifikation nicht nötig ist.

Handelt es sich bei der Gegenstelle um eine Scalance S, dann entnehmen sie die Remote ID der Projektierung der Scalance S und tragen sie diese als Remote ID im MD740-1 ein. Die Eingabe einer Lokale ID ist nicht erforderlich.

Pre-Shared Secret Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei verschlüsselt das MD740-1 die Datagramme, die es zur Gegenstelle, dem „Tunnelende“, sendet, mit einer verabredeten Zeichenfolge.

Um diesen verabredeten Schlüssel dem MD740-1 zur Verfügung zu stellen, gehen Sie wie folgt vor:

1. *Konfigurieren* klicken.

   Folge: Der nachfolgend abgebildete Bildschirm erscheint:



Abbildung 4-18

2. Ins Eingabefeld *Pre-Shared Secret Key (PSK)* die verabredete Zeichenfolge eintragen. Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

3. *Zurück* klicken.

Hinweis

Pre-Shared Secret Key kann nicht mit dynamischen (%any) IP-Adressen verwendet werden, nur feste IP-Adressen oder Hostnamen auf beiden Seiten werden unterstützt.

Hinweis

Lokale ID und Remote ID (siehe *X.509 Zertifikat*) müssen bei Verwendung von *Pre-Shared Secret Key* und nur einer Tunnelverbindung nicht eingegeben werden.

Verbindungstyp

Es stehen zur Auswahl:

- Tunnel (Netz ← → Netz)
- Transport (Host ← → Host)
- Transport (L2TP Microsoft Windows)
- Transport (L2TP SSH Sentinel)

Tunnel (Netz ← → Netz)

Dieser Verbindungstyp eignet sich in jedem Fall und ist der sicherste. In diesem Modus werden die zu übertragenden IP-Datagramme vollkommen verschlüsselt und mit einem neuen Header versehen zur VPN-Gateway der Gegenstelle, dem „Tunnelende", gesendet. Dort werden die übertragenen Datagramme entschlüsselt und aus ihnen die ursprünglichen Datagramme wiederhergestellt. Diese werden dann zum Zielrechner weitergeleitet.

Transport (Host ← → Host)

Bei diesem Verbindungstyp werden nur die Daten der IP-Pakete verschlüsselt. Die IP Header Informationen bleiben unverschlüsselt.

Transport (L2TP Microsoft Windows)

Ist beim entfernten Rechner dieser Verbindungstyp aktiviert, dann setzen Sie das MD740-1 auch auf Transport (*L2TP Microsoft Windows*). Dann arbeitet das MD740-1 entsprechend. Das heißt, innerhalb der IPsec-Transport-Verbindung schafft das L2TP/PPP Protokoll einen Tunnel. Dem lokal angeschlossenen L2TP-Rechner wird seine IP-Adresse vom MD740-1 dynamisch zugewiesen.

Bei Auswahl des Verbindungstyps *Transport (L2TP Microsoft Windows)* setzen Sie *Perfect Forward Secrecy (PFS)* auf *Nein*. Aktivieren Sie auch den L2TP-Server.

Hinweis

Sobald unter Windows die IPsec/L2TP-Verbindung gestartet wird, erscheint ein Dialogfeld, das nach Benutzername und Login fragt. Sie können dort beliebige Einträge machen, denn die Authentifizierung erfolgt bereits über die X.509 Zertifikate, so dass das MD740-1 diese Eingaben ignoriert.

Transport (L2TP SSH Sentinel)

Ist beim lokal angeschlossenen Rechner dieser Verbindungstyp aktiviert, dann setzen Sie das MD740-1 auch auf *Transport (L2TP SSH Sentinel)*. Dann arbeitet das MD740-1 entsprechend. Das heißt, innerhalb der IPsec-Transport-Verbindung schafft das L2TP/PPP Protokoll einen Tunnel. Dem lokal angeschlossenen L2PT-Rechner wird seine IP-Adresse vom MD740-1 dynamisch zugewiesen. Aktivieren Sie auch den L2TP-Server.

Verbindungsinitiierung

Es gibt 2 Möglichkeiten:

- Starte die Verbindung zur Gegenstelle
- Warte auf Gegenstelle

Starte die Verbindung zur Gegenstelle
In diesem Fall initiiert das lokale MD740-1 die Verbindung zur Gegenstelle. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) muss die feste IP-Adresse der Gegenstelle oder deren Domain Name eingetragen sein.

Warte auf Gegenstelle
In diesem Fall ist das lokale MD740-1 bereit, die Verbindung anzunehmen, die eine entfernte Gegenstelle aktiv zum lokalen MD740-1 initiiert und aufbaut. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) kann eingetragen sein: **%any**

Baut ausschließlich eine bestimmte Gegenstelle mit fester IP-Adresse die Verbindung auf, können Sie sicherheitshalber deren IP-Adresse oder Hostnamen angeben.

Hinweis

Damit eine Verbindung zum MD740-1 aufgebaut werden kann, benötigt das MD740-1 eine feste IP-Adresse, durch den Provider oder durch Nutzung eines DynDNS-Service.

Hinweis

Der Verbindungsaufbau von einer entfernten Gegenstelle zum MD740-1 wird in vielen GSM/GPRS-Netzen nicht unterstützt.

Weitere IKE Einstellungen: Konfigurieren

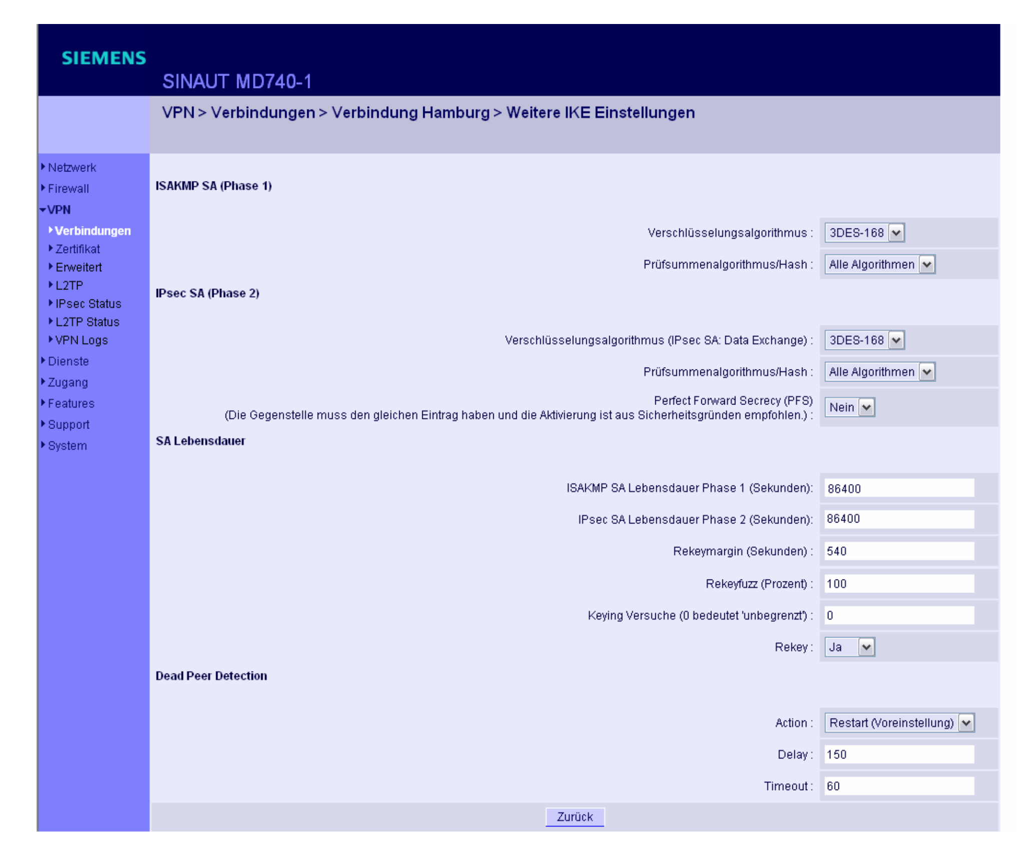


Abbildung 4-19

ISAKMP SA (Phase 1)

Authentisierungsverfahren - siehe *Authentisierungsverfahren,* Seite 58

Verschlüsselungsalgorithmus

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

3DES-168 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Grundsätzlich gilt Folgendes:
Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das relativ neue Verfahren AES-256 gilt daher als am sichersten, ist aber noch nicht so verbreitet.
Der Verschlüsselungsvorgang ist um so zeitaufwendiger, je länger der Schlüssel ist. Dieser Gesichtspunkt spielt für das MD740-1 keine Rolle, weil es mit Hardware-basierter Verschlüsselungstechnik arbeitet. Jedoch könnte dieser Aspekt für die Gegenstelle eine Rolle spielen.

Der zur Auswahl stehende, mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.

Prüfsummenalgorithmus/Hash

Lassen Sie die Einstellung auf *Alle Algorithmen* stehen. Dann spielt es keine Rolle, ob die Gegenstelle mit MD5 oder SHA-1 arbeitet.

IPsec SA (Phase 2)

Im Unterschied zu ISAKMP SA (Phase 1) (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Die können sich von denen des Schlüsselaustauschs unterscheiden, müssen aber nicht.

Verschlüsselungsalgorithmus (IPsec SA: Data Exchange)

Siehe oben.

Prüfsummenalgorithmus/Hash

Siehe oben.

Perfect Forward Secrecy (PFS)

Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten.
Nur wenn die Gegenstelle PFS unterstützt, wählen Sie *Ja*.

Bei Auswahl des Verbindungstyps *Transport (L2TP Microsoft Windows)* setzen Sie *Perfect Forward Secrecy (PFS)* auf *Nein*.

SA Lebensdauer

Die Schlüssel einer IPsec Verbindung werden in bestimmten Abständen erneuert, um den Aufwand eines Angriffs auf eine IPsec Verbindung zu erhöhen.

ISAKMP SA Lebensdauer (Sekunden)
Lebensdauer der für die ISAKMP SA vereinbarten Schlüssel in Sekunden. Die Werkseinstellung sind 86400 Sekunden (24 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

IPsec SA Lebensdauer (Sekunden)
Lebensdauer der für die IPsec SA vereinbarten Schlüssel in Sekunden. Die Werkseinstellung sind 86400 Sekunden (24 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

Rekeymargin (Sekunden)
Minimale Zeitspanne vor Ablauf der alten Schlüssel, innerhalb der ein neuer Schlüssel erzeugt werden soll. Werkseinstellung: 540 Sekunden (9 Minuten)

Rekeyfuzz (Prozent)
Maximum in Prozent, um das das Rekey Margin zufällig vergrößert werden soll. Dies dient dazu, den Schlüsselaustausch auf Maschinen mit vielen VPN Verbindungen zeitversetzt stattfinden zu lassen. Werkseinstellung: 100 Prozent.

Keying Versuche (0 bedeutet unbegrenzt)
Anzahl der Versuche, die unternommen werden sollen, neue Schlüssel mit der Gegenstelle zu vereinbaren. Der Wert 0 bedeutet bei Verbindungen, die das MD740-1 initiieren soll, unendlich viele Versuche, ansonsten 5 Versuche.

Rekey (Ja / Nein)
Bei *Ja* wird diese Seite versuchen, einen neuen Schlüssel zu vereinbaren, wenn die Gültigkeit des alten abgelaufen ist.

Dead Peer Detection

Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss. Ohne DPD muss je nach Konfiguration bis zum Ablauf der SA Lebensdauer gewartet oder die Verbindung manuell neu initiiert werden.

Action: Clear / Hold / Restart (Voreinstellung)
Bei **Hold** (Halten) wird versucht, die IPsec Verbindung neu aufzubauen, wenn diese für tot erklärt wurde, aber nur, wenn das lokal angeschlossene Netz versucht, Daten zur Gegenstelle zu senden.
Bei **Restart** (erneut starten) wird versucht, die IPsec Verbindung neu aufzubauen, wenn diese für tot erklärt wurde, unabhängig von der Übertragung von Nutzdaten.
Bei **Clear** (Löschen) wird nicht versucht, die Verbindung erneut aufzubauen.
Die Werkseinstellung ist **Restart**.

Delay
Zeitspanne in Sekunden, nach welcher DPD-Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist. Werkseinstellung: 300 Sekunden.

Timeout
Zeitspanne in Sekunden, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die DPD-Anfragen keine Antwort erfolgte. Werkseinstellung: 120 Sekunden.

Tunnel Einstellungen

Die Adresse des lokalen Netzes

Die dazugehörige Netzmaske

Mit diesen beiden Angaben geben Sie die Adresse des Clients (Netz oder Rechner) an, der lokal direkt am MD740-1 angeschlossen ist und den das MD740-1 schützt. Diese Adresse bezeichnet den lokalen Endpunkt der Verbindung.

Beispiel:

Ist am MD740-1 der Rechner angeschlossen, den Sie auch zur Konfiguration des Gerätes benutzen, dann könnten diese Angaben lauten:

Adresse des lokalen Netzes: 192.168.1.1

Die dazugehörige Netzmaske: 255.255.255.0

Siehe auch *Kapitel 4.11.*

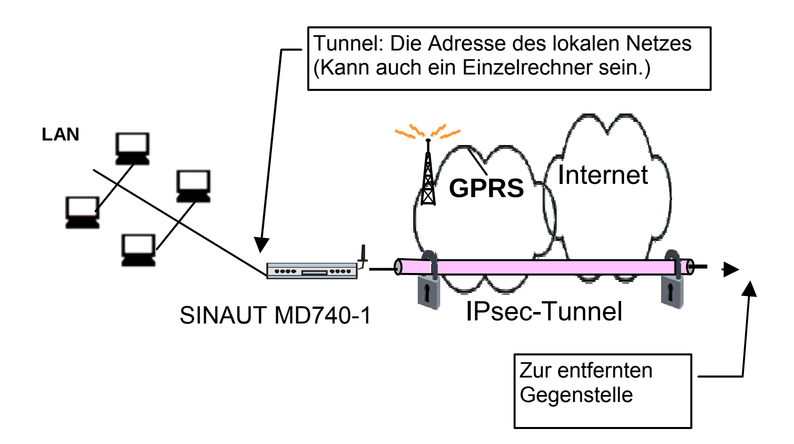


Abbildung 4-20 Lokale Geräte und Adressen

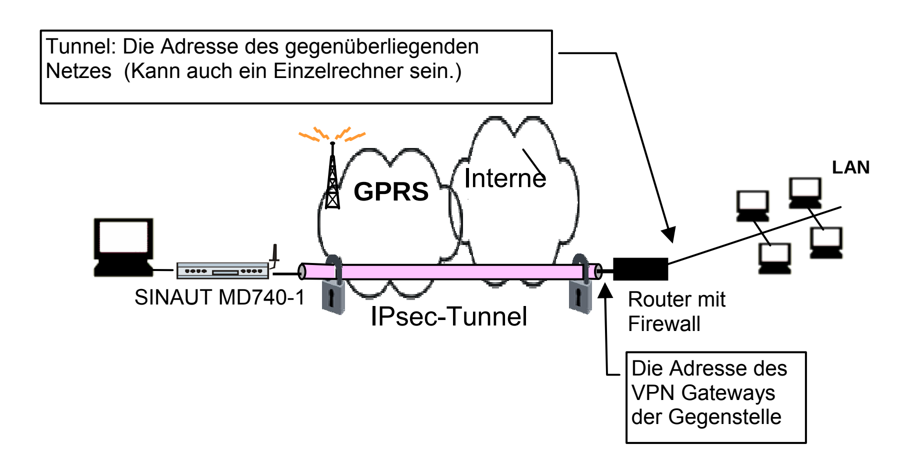


Abbildung 4-21 Geräte und Adressen der Gegenstelle

Die Adresse des gegenüberliegenden Netzes

Die dazugehörige Netzmaske

Mit diesen beiden Angaben geben Sie die Adresse des Netzes an, in dem sich der entfernte Kommunikationspartner befindet. Diese Adresse kann auch die eines Rechners sein, der direkt am VPN-Gateway angeschlossen ist.

Firewall eingehend (ungesicherter Port), Firewall ausgehend (gesicherter Port)

Während die unter dem Menüpunkt *Firewall* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe Kapitel 4.3.1), beziehen sich die Einstellungen hier ausschließlich auf die hier definierte VPN-Verbindung. Das bedeutet praktisch: Haben Sie mehrere VPN-Verbindungen definiert, können Sie für jede einzelne den Zugriff von außen oder von innen beschränken. Versuche, die Beschränkungen zu übergehen, können Sie ins Log protokollieren lassen.

Hinweis

Gemäß werksseitiger Voreinstellung ist die VPN-Firewall so eingestellt, dass für diese VPN-Verbindung alles zugelassen ist.
Für jede einzelne VPN-Verbindung gelten aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind (siehe Kapitel 4.3.5).

Hinweis

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Firewall-Regel setzen oder löschen

Um eine Firewall-Regel zu setzen oder zu löschen gehen Sie genauso vor wie oben beschrieben (siehe Kapitel 4.3.1 und Kapitel 4.3.2).

Wie dort haben Sie bei den Angaben folgende Möglichkeiten:

Protokoll:

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von / nach IP:

IP-Adresse oder -Adressenbereich. **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 4.10.

Von / nach Port:

(wird nur ausgewertet bei den Protokollen TCP und UDP)
any bezeichnet jeden beliebigen Port.
startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben
(z. B. 110 für pop3 oder pop3 für 110).

Aktion:

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.

Log:

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen oder nicht - *Log* auf *Nein* setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge befolgt.

4.4.2 VPN → Maschinenzertifikat



Abbildung 4-22

Zertifikat

Zeigt das aktuell importierte X.509-Zertifikat an, mit dem sich das MD740-1 gegenüber anderen VPN-Gateways ausweist.
Nach dem Import eines Zertifikats werden hier folgende Informationen angezeigt:

Subject

Der Besitzer, auf den das Zertifikat ausgestellt ist.

Issuer

Die Beglaubigungsstelle, die das Zertifikat unterschrieben hat.

C: Land (Country)

ST: Bundesland (State)

L: Stadt (Location)

O: Organisation

OU: Abteilung (Organisation Unit)

CN: Hostname, allgemeiner Name (Common Name)

MD5, SHA1 Fingerprint

Fingerabdruck des Zertifikats. Anhand des Fingerabdrucks (Fingerprints) eines Zertifikats lässt sich durch Vergleich feststellen, ob dieses echt ist. Erhalten Sie ein Zertifikat, so können Sie mit dem Erzeuger des Zertifikats Kontakt aufnehmen und mit ihm den Fingerabdruck vergleichen, um die Echtheit zu überprüfen. Windows zeigt an dieser Stelle den Fingerabdruck im SHA1-Format an.

notBefore, notAfter

Gültigkeitszeitraum des Zertifikats. Wird vom MD740-1 mangels einer eingebauten Uhr ignoriert.

Die importierte Zertifikatsdatei (Dateinamen-Erweiterung *.p12 oder *.pfx) enthält neben den oben angegebenen Informationen die beiden Schlüssel, den öffentlichen zum Verschlüsseln, den privaten zum Entschlüsseln. Der zugehörige öffentliche Schlüssel kann an beliebig viele Verbindungspartner vergeben werden, so dass diese verschlüsselte Daten senden können.

In Abstimmung mit der Gegenstelle muss das Zertifikat als .cer- oder .pem-Datei dem Bediener der entfernten Gegenstelle zur Verfügung gestellt werden - z. B. durch persönliche Übergabe oder per E-Mail. Wenn Ihnen kein sicherer Übertragungsweg zur Verfügung steht, sollten Sie anschließend den vom MD740-1 angezeigten Fingerabdruck über einen sicheren Weg vergleichen.

Es kann nur eine Zertifikats-Datei (PKCS#12-Datei) ins Gerät importiert werden.

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues Zertifikat

Voraussetzung:
Die Zertifikatsdatei (Dateiname = *.p12 oder *.pfx) ist generiert und auf dem angeschlossenen Rechner gespeichert.

1. *Durchsuchen...* klicken, um die Datei zu selektieren
2. In das Feld *Passwort* geben Sie das Passwort ein, mit dem der private Schlüssel der PKCS#12-Datei geschützt ist.
3. *Importieren* klicken.
4. Abschließend *Übernehmen* klicken.

4.4.3 VPN → Erweiterte Einstellungen

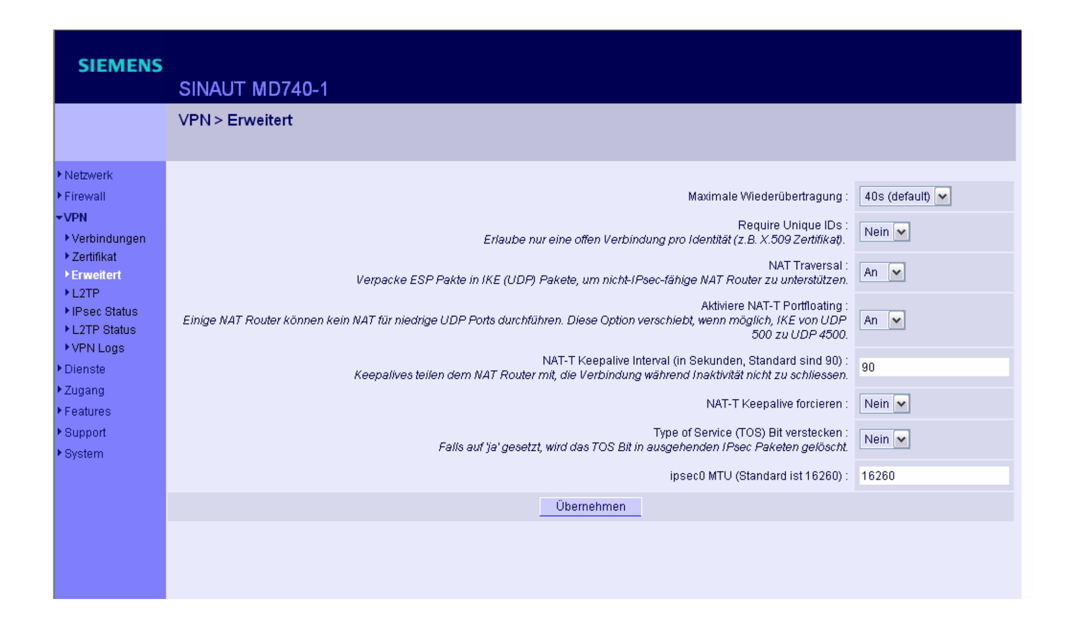


Abbildung 4-23

Maximum Retransmission

Schlägt der Versuch fehl, einen VPN-Tunnel aufzubauen, unternimmt das Gerät weitere Versuche, den Tunnel herzustellen, so lange, bis der gewünschte VPN-Tunnel aufgebaut ist. Die Versuche finden in sich verlängernden Zeitabständen statt. *Maximum Retransmission* legt fest, wie groß diese Zeitabstände maximal werden.

Require Unique IDs: Ja / Nein

Bei Ja: Je Identität (d. h. je X.509 Zertifikat) wird nur eine einzige offene Verbindung zugelassen.

NAT Traversal: Ein / Aus

Bei Ein: ESP Traffic in IKE (UDP) Datenpakte einkapseln, um NAT-Router, die IPsec nicht kennen, passieren zu können.

Enable NAT-T Portfloating: Ein / Aus

Bei Ein: Einige NAT-Router sind nicht in der Lage, bei Datenverkehr, die von UDP-Ports mit tiefen Nummern ausgehen, NAT durchzuführen. Bei Aktivierung dieser Option wird IKE von UDP 500 auf UDP 4500 gesetzt, wenn möglich.

NAT-T Keepalive Interval

(In Sekunden. Standardeinstellung: 300)
Keepalives signalisieren dem NAT-Router, die Verbindung nicht zu schließen, auch wenn sie nicht aktiv ist.

Force NAT-T Keepalive: Ja / Nein

Bei Ja: Bei Aushandlung der Verbindungsparameter wird darauf bestanden, dass während der Verbindung NAT-T Keepalive Pakete ausgetauscht werden.

Hide Type of Service (TOS) Bit: Ja / Nein

Bei Ja: Bei IPsec Ausgabe wird das TOS-Bit gelöscht.

IPsec 0 MTU (default is 16260)

Reserviert. Wert nicht ändern.

4.4.4 VPN → L2TP



Abbildung 4-24

Starte L2TP Server für IPsec/L2TP? Ja / Nein

Wollen Sie eine L2TP-Verbindung ermöglichen, setzen Sie diesen Schalter auf *Ja*.

Innerhalb der IPsec Transport-Verbindung beinhaltet die L2TP Verbindung wiederum eine PPP-Verbindung. Im Ergebnis entsteht dadurch praktisch eine Art Tunnel zwischen 2 Netzen. Dabei teilt das MD740-1 der Gegenstelle über PPP mit, welche Adressen benutzt werden: für sich selber und die entfernte Gegenstelle.

Lokale IP für L2TP Verbindungen

Nach dem obigen Screenshot teilt das MD740-1 der Gegenstelle mit, es habe die Adresse 10.106.106.1.

Zuweisung von IPs für L2TP Gegenstellen

Nach dem obigen Screenshot teilt das MD740-1 der Gegenstelle mit, diese habe die Adressen ab 10.106.106.2 (bei einem einzigen Rechner) bis 10.106.106.254 (bei mehreren Rechnern).

4.4.5 VPN → IPsec Status



Abbildung 4-25

Informiert über den Status der IPsec-Verbindungen. Links sind die Namen der VPN-Verbindungen aufgelistet, rechts daneben wird jeweils deren aktueller Status angezeigt.

GATEWAY

bezeichnet die kommunizierenden VPN-Gateways.

TRAFFIC

bezeichnet Rechner bzw. Netze, die über die VPN-Gateways kommunizieren.

ID

bezeichnet den Distinguished Name (DN) eines X.509-Zertifikats.

ISAKMP Status

ISAKMP Status (Internet security association and key management protocol) ist mit „established“ angegeben, wenn die beiden beteiligten VPN-Gateways einen Kanal zum Schlüsselaustausch aufgebaut haben. In diesem Fall konnten sie einander kontaktieren, und alle Einträge bis einschließlich „ISAKMP SA“ auf der Konfigurationsseite der Verbindung waren korrekt.

IPsec Status

IPsec Status ist mit „established“ angegeben, wenn die IPsec-Verschlüsselung bei der Kommunikation aktiviert ist. In diesem Fall waren auch die Angaben unter „IPsec SA“ und „Tunnel-Einstellungen“ korrekt.

Bei Problemen empfiehlt es sich, in die VPN-Logs des Rechners zu schauen, zu dem die Verbindung aufgebaut wurde. Denn der initiierende Rechner bekommt aus Sicherheitsgründen keine ausführlichen Fehlermeldungen zugesandt.

Die Anzeige:

ISAKMP SA established, IPsec State: WAITING

bedeutet:
Die Authentifizierung war erfolgreich, jedoch stimmten die anderen Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?

Die Anzeige:

IPsec State: IPsec SA established

bedeutet:
Die VPN-Verbindung ist erfolgreich aufgebaut und kann genutzt werden. Sollte dies dennoch nicht der Fall sein, dann gibt es Probleme mit dem VPN-Gateway der Gegenstelle. In diesem Fall den Verbindungsnamen anklicken und dann *Übernehmen* klicken, um die Verbindung erneut aufzubauen.

4.4.6 VPN → L2TP Status



Abbildung 4-26

Nur Anzeige:

Informiert über den L2TP-Status, wenn dieser als Verbindungstyp gewählt ist. Siehe *Kapitel 4.4.1.*

Ist dieser Verbindungstyp nicht gewählt, sehen Sie die abgebildete Anzeige VPN → VPN Logs.

4.4.7 VPN → VPN Logs

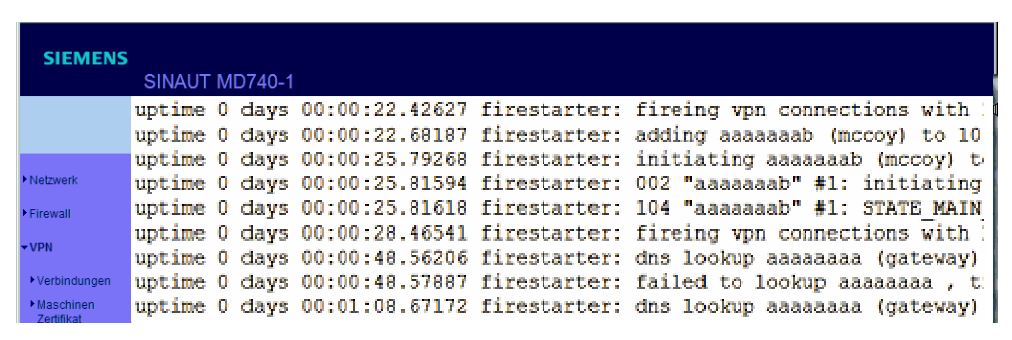


Abbildung 4-27

Nur Anzeige:

Listet alle VPN-Ereignisse auf.

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

4.5 Menü Dienste

4.5.1 Dienste → DNS

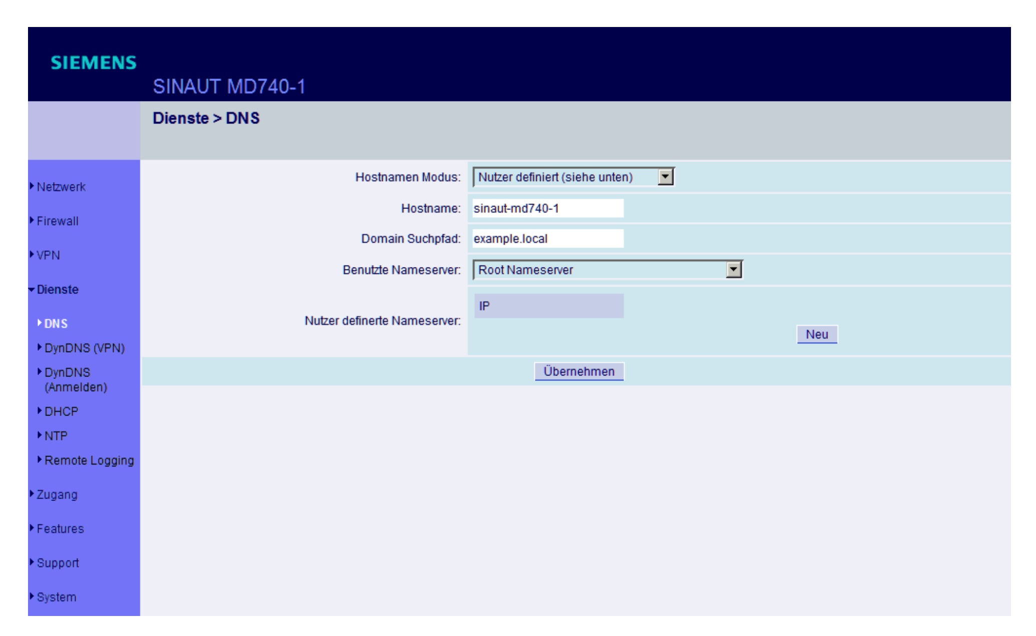


Abbildung 4-28

Soll das MD740-1 eine Verbindung zu einer Gegenstelle aufbauen (z. B. VPN-Gateway oder NTP-Server), muss ihm die IP-Adresse dieser Gegenstelle bekannt sein. Wird ihm die Adresse in Form einer Domain-Adresse angegeben (d. h. in der Form www.abc.xyz.de), dann muss das Gerät auf einem Domain Name Server (DNS) nachschlagen, welche IP-Adresse sich hinter der Domain-Adresse verbirgt.

Sie können die lokal angeschlossenen Clients so konfigurieren, dass sie das MD740-1 zur Auflösung von Hostnamen in IP-Adressen benutzen können. Siehe dazu im Abschnitt 4.5.4 die Beschreibung der IP-Konfiguration bei Windows-Clients.

Hostnamen Modus

Mit *Hostnamen Modus* und *Hostname* können Sie dem MD740-1 einen Namen geben. Dieser wird dann z. B. beim Einloggen per SSH angezeigt. Eine Namensgebung erleichtert die Administration mehrerer MD740-1-Geräte.

Nutzer definiert (siehe unten)

(Standard) Der im Feld *Hostname* eingetragene Name wird als Name für das MD740-1 gesetzt.

Provider definiert (z. B. via DHCP)

Ist ein externes Setzen des Hostnamens ermöglicht wie z. B. bei DHCP, dann wird der vom Provider übermittelte Name für das MD740-1 gesetzt.

Hostname

Ist unter *Hostnamen Modus* die Option *Nutzer definiert* ausgewählt, dann tragen Sie hier den Namen ein, den das MD740-1 erhalten soll.

Sonst, d. h. wenn unter *Hostnamen Modus* die Option *Provider definiert* (z. B. via DHCP) ausgewählt ist, dann wird ein Eintrag in diesem Feld ignoriert.

Domain-Suchpfad

Erleichtert dem Benutzer die Eingabe eines Domain-Namens: Gibt der Benutzer den Domain-Namen gekürzt ein, ergänzt das MD740-1 seine Eingabe um das angegebene Domain-Suffix, das hier unter Domain-Suchpfad festgelegt wird.

Benutzte Nameserver

Möglichkeiten: Root Nameserver / Provider definiert / Nutzer definiert

Root Nameserver
Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im MD740-1 gespeichert sind. Diese Adressen ändern sich selten. Diese Einstellung sollte nur gewählt werden, wenn die alternativen Einstellungen nicht funktionieren.

Provider definiert (z. B. via PPPoE oder DHCP)
Es wird der Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. Diese Einstellung können Sie bei aktiviertem DHCP wählen (siehe *Dienste → DHCP*).

Nutzer definiert (unten stehende Liste)
Ist diese Einstellung gewählt, nimmt das MD740-1 mit den Domain Name Servern Verbindung auf, die in der Liste *Nutzer definierte Nameserver* aufgeführt sind.

Nutzer definierte Nameserver

Haben Sie unter *Benutzte Nameserver* die Option *Nutzer definiert* eingestellt, konfigurieren Sie in dieser Liste die IP-Adressen der zu benutzenden Domain Name Server.

Hinweis

Damit die lokal angeschlossenen Clients die Auflösung von Hostnamen in IP-Adressen vom MD740-1 beziehen können, müssen Sie bei den Clients die lokale IP-Adresse des MD740-1 als *Bevorzugten DNS-Server* festlegen.

Siehe dazu im Abschnitt 4.5.4 die Beschreibung der IP-Konfiguration bei Windows-Clients.

4.5.2 Dienste → DynDNS Überwachung

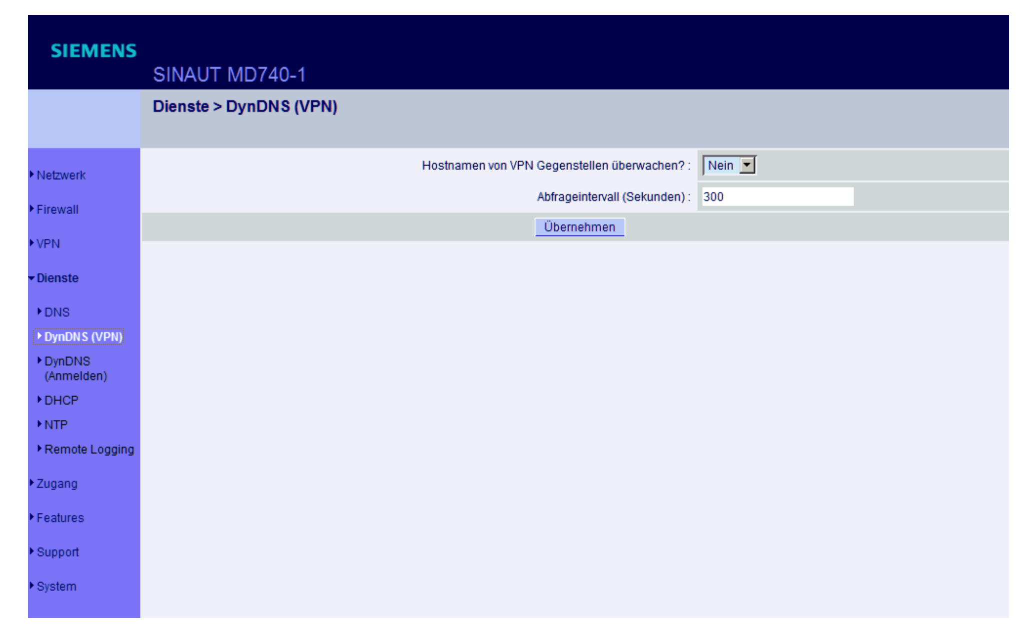


Abbildung 4-29

Hostnamen von VPN Gegenstellen überwachen? Ja / Nein

Ist dem MD740-1 die Adresse der VPN-Gegenstelle als Hostname angegeben (siehe Kapitel 4.4.1) und ist dieser Domain Name von einem DynDNS Service zugeteilt, dann kann das MD740-1 regelmäßig überprüfen, ob beim betreffenden DynDNS keine Änderung erfolgt ist. Falls ja, wird die VPN-Verbindung zu der neuen IP-Adresse aufgebaut.

Abfrageintervall (Sekunden)

Standard: 300 (Sekunden)

4.5.3 Dienste → DynDNS (Anmelden)

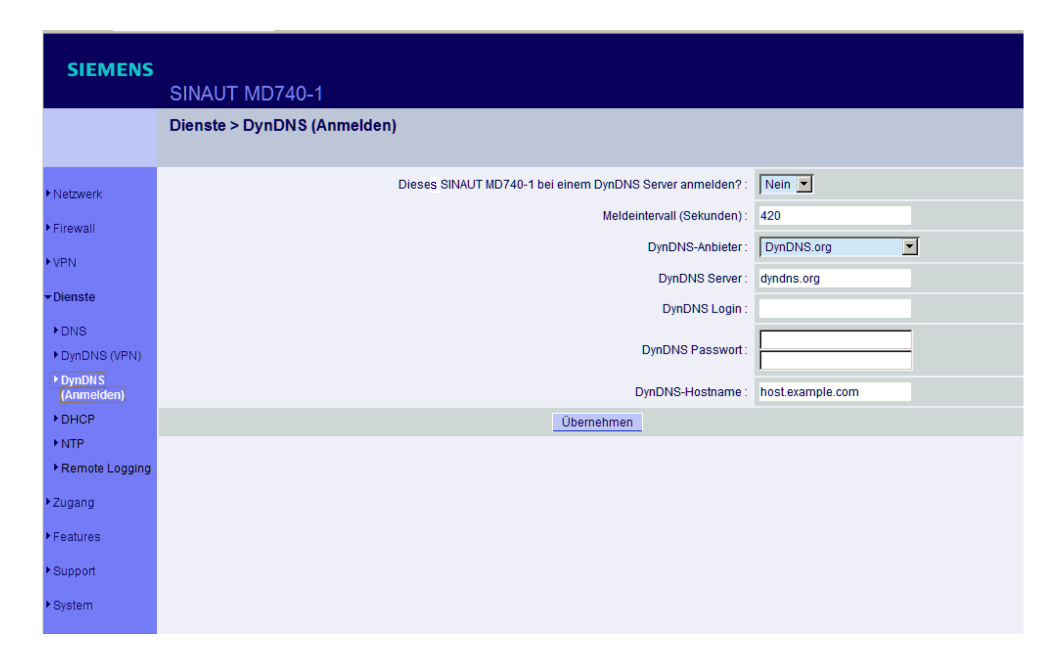


Abbildung 4-30

Zum Aufbau von VPN-Verbindungen muss mindestens die IP-Adresse eines der Partner bekannt sein, damit diese miteinander Kontakt aufnehmen können. Diese Bedingung ist nicht erfüllt, wenn beide Teilnehmer ihre IP-Adressen dynamisch von ihrem Internet Service Provider zugewiesen bekommen. In diesem Fall kann aber ein DynDNS-Service wie z. B. DynDNS.org oder DNS4BIZ.com helfen. Bei einem DynDNS-Service wird die jeweils gültige IP-Adresse unter einem festen Namen registriert wird. Siehe auch Kapitel 1.3.

Sofern Sie für einen vom MD740-1 unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Dieses SINAUT MD740-1 bei einem DynDNS Server anmelden?

Wählen Sie *Ja*, wenn Sie beim DynDNS-Anbieter entsprechend registriert sind und das MD740-1 den Service benutzen soll. Dann meldet das MD740-1 die aktuelle IP-Adresse, die dem eigenen Internet-Anschluss vom Internet Service Provider zugewiesen ist, an den DynDNS Service

Meldeintervall (Sekunden)

Standard: 420 (Sekunden).

Immer wenn die IP-Adresse des eigenen Internet-Anschlusses geändert wird, informiert das MD740-1 den DynDNS Service über die neue IP-Adresse. Aus Zuverlässigkeitsgründen erfolgt diese Meldung zusätzlich in dem hier festgelegten Zeitintervall.

DynDNS Anbieter

Die zur Auswahl gestellten Anbieter unterstützen das Protokoll, das auch das MD740-1 unterstützt.

Geben Sie den Namen des Anbieters an, bei dem Sie registriert sind, z. B. DynDNS.org

DynDNS Server

Name des Servers des oben ausgewählten DynDNS-Anbieters, z. B.: *dyndns.org*

DynDNS Login, DynDNS Passwort

Geben Sie hier den Benutzernamen und das Passwort ein, das Ihnen vom DynDNS-Anbieter zugeteilt worden ist.

DynDNS Hostname

Der für dieses MD740-1 gewählte Hostname beim DynDNS-Service - sofern Sie einen DynDNS-Dienst benutzen und oben die entsprechenden Angaben gemacht haben.

4.5.4 Dienste → DHCP

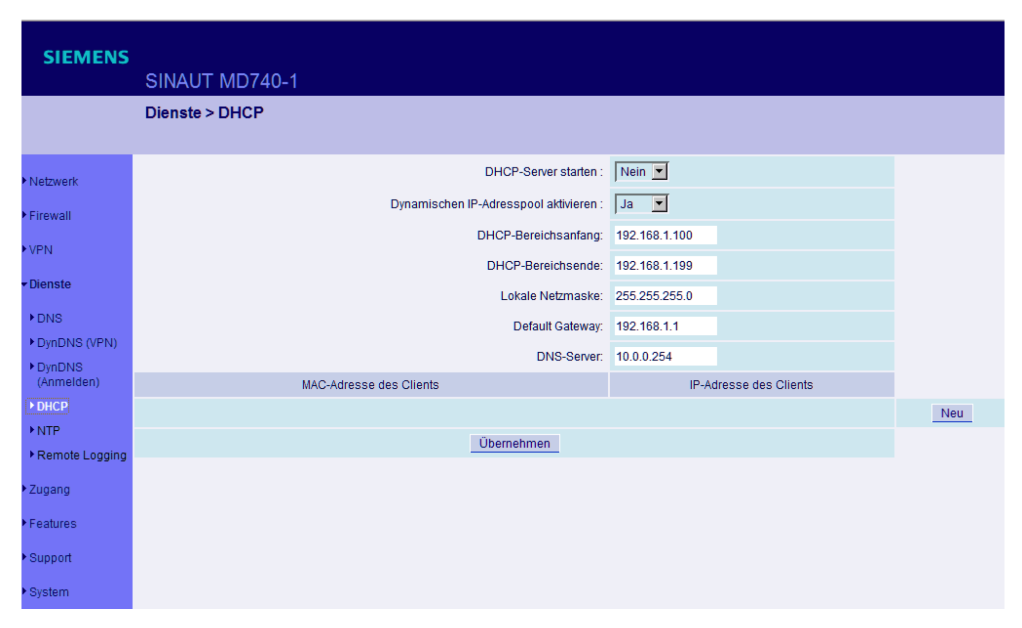


Abbildung 4-31

(DHCP = Dynamic Host Configuration Protocol) Diese Funktion ordnet den lokal am MD740-1 angeschlossenen Clients automatisch die gebotene Netzwerkkonfiguration zu (IP-Adresse und Subnetzmaske).

DHCP-Server starten

Setzen Sie diesen Schalter auf *Ja*, wenn Sie diese Funktion aktivieren wollen.

Dynamischen IP-Adresspool aktivieren

Setzen Sie diesen Schalter auf *Ja*, wenn sie den durch DHCP-Bereichsanfang bzw. DHCP-Bereichsende gewählten IP-Adresspool verwenden wollen.

Setzen Sie diesen Schalter auf *Nein*, wenn nur statische Zuweisungen anhand der MAC-Adresse vorgenommen werden sollen (siehe unten).

Optionen:

Bei aktiviertem DHCP-Server und aktiviertem dynamischem IP-Adresspool können Sie die Netzwerkparameter angeben, die vom Client benutzt werden sollen.

DHCP-Bereichsanfang: DHCP-Bereichsende:	Anfang und Ende des Adressbereichs, aus dem der DHCP-Server des MD740-1 den lokal angeschlossenen Clients IP-Adressen zuweisen soll.
Lokale Netzmaske:	Voreingestellt ist: 255.255.255.0
Default-Gateway:	Legt fest, welche IP-Adresse beim Client als Standardgateway benutzt wird. In der Regel ist das die lokale IP-Adresse des MD740-1.
DNS-Server:	Legt fest, von wo Clients die Auflösung von Hostnamen in IP-Adressen beziehen. Wenn der DNS-Dienst des MD740-1 aktiviert ist, kann das die lokale IP-Adresse des MD740-1 sein.

Tabelle 4-4

MAC-Adresse des Clients / IP-Adresse des Clients

Die MAC-Adresse Ihres Clients finden Sie wie folgt heraus:

Windows 95/98/ME: Starten Sie "winipcfg" in einer DOS-Box

Windows NT/2000/XP: Starten Sie "ipconfig /all" in einer Eingabeaufforderung. Die MAC-Adresse wird als "Physikalische Adresse" angezeigt.

Linux: Rufen sie in einer Shell "/sbin/ifconfig" oder "ip link show" auf

Zuweisung löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*, dann *Übernehmen*.

Zuweisung hinzufügen

Wollen Sie eine neuen Zuweisung hinzufügen, klicken Sie *Neu*.

Geben Sie die Daten der Zuweisung an (s. u.) und klicken Sie *Übernehmen*.

Geben Sie ein:

MAC-Adresse des Clients
Die MAC-Adresse (ohne Leerzeichen oder Bindestriche) des Clients.

IP-Adresse des Clients
Die statische IP, die der MAC-Adresse des Clients zugewiesen werden soll.

Hinweis

- Die statischen Zuweisungen haben Vorrang vor dem dynamischen IP-Adresspool.
- Statische Zuweisungen dürfen sich nicht mit dem dynamischen IP-Adresspool überlappen.
- Eine IP darf nicht in mehreren statischen Zuweisungen verwendet werden, ansonsten wird diese IP mehreren MAC-Adressen zugeordnet.
- Es darf nur ein DHCP-Server pro Subnetz verwendet werden.
- Wenn Sie den DHCP-Server des MD740-1 starten, müssen Sie die lokal angeschlossenen Clients so konfigurieren, dass sie ihre IP-Adressen automatisch beziehen (s. u.).

IP-Konfiguration bei Windows-Clients

Dazu klicken Sie unter Windows XP *Start, Systemsteuerung, Netzwerkverbindungen*: Symbol des LAN-Adapters mit der rechten Maustaste klicken und im Kontextmenü *Eigenschaften* klicken. Im Dialogfeld *Eigenschaften von LAN-Verbindung* lokales Netz auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag *Internetprotokoll (TCP/IP)* markieren und dann die Schaltfläche *Eigenschaften* klicken.

Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* die gebotenen Angaben bzw. Einstellungen machen.

4.5.5 Dienste → NTP

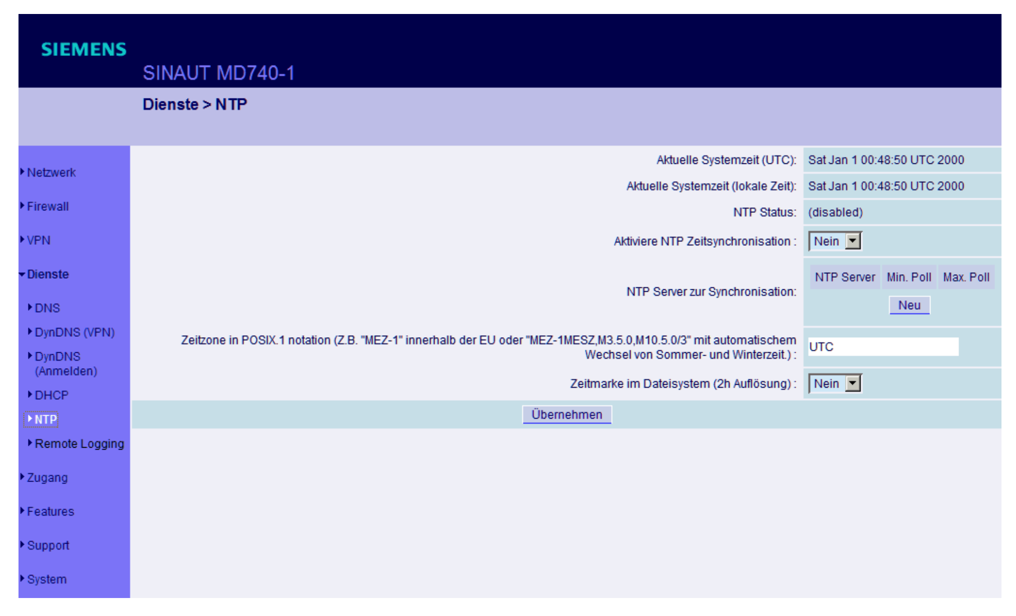


Abbildung 4-32

(NTP = Network Time Protocol)

Aktuelle Systemzeit (UTC)

Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC). Wenn die *NTP Zeitsynchronisation* noch nicht aktiviert ist (s. u.) und *Zeitmarken im Dateisystem* deaktiviert sind, beginnt die Uhr mit dem 1. Januar 2000.

Aktuelle Systemzeit (lokale Zeit)

Soll die eventuell abweichende aktuelle Ortszeit angezeigt werden, müssen Sie unter *Zeitzone in POSIX.1 Notation...* den entsprechenden Eintrag machen.

NTP Status

Anzeige des aktuellen NTP-Status

Aktiviere NTP Zeitsynchronisation: Ja / Nein

Sobald das NTP aktiviert ist, bezieht das MD740-1 die Zeit aus dem Internet und zeigt diese als aktuelle Systemzeit an. Die Synchronisation kann einige Sekunden dauern.

Nur wenn dieser Schalter auf *Ja* steht und unter *NTP Server zur Synchronisation* (s. u.) mindestens 1 Zeitserver angegeben ist, wird die aktuelle Systemzeit zur Verfügung gestellt.

NTP Server zur Synchronisation

NTP Server

Geben Sie hier einen oder mehrere Zeitserver an, von denen das MD740-1 die aktuelle Zeitangabe beziehen soll. Falls Sie mehrere Zeitserver angeben, verbindet sich das MD740-1 automatisch mit allen, um die aktuelle Zeit zu ermitteln.

Das MD740-1 stellt auch den angeschlossenen Rechnern die NTP-Zeit zur Verfügung.

➲ Geben Sie die IP-Adressen (statt der Hostnamen) der gewünschten Zeitserver ein.

➲ Genutzte NTP Server müssen kompatibel sein zum NTP daemon des NTP Referenzprojektes (www.ntp.org).

Min. Poll / Max. Poll

Die Zeitsynchronisation erfolgt zyklisch. Geben Sie hier das Intervall an, in dem die Abfrage stattfinden soll (Poll-Intervall).

Der NTP-Client wählt das Poll-Intervall dynamisch zwischen beiden Werten. Bitte achten Sie darauf, den minimalen Wert kleiner als den maximalen Wert einzugeben.

Zeitzone in POSIX.1 Notation...

Soll oben unter *Aktuelle Systemzeit* nicht die aktuelle Greenwich-Zeit angezeigt werden, sondern Ihre aktuelle Ortszeit (= abweichend von der Greenwich-Zeit), dann tragen Sie hier ein, um wie viel Stunden bei Ihnen die Zeit voraus bzw. zurück ist.

Beispiele:

In Hamburg ist die Uhrzeit der Greenwich-Zeit um 1 Stunde voraus. Also tragen Sie ein: MEZ-1

Wünschen Sie die Anzeige der MEZ-Uhrzeit (= gültig für Deutschland) mit automatischer Umschaltung auf Sommer- bzw. Winterzeit geben Sie ein:

MEZ-1MESZ,M3.5.0,M10.5.0/3

Bedeutung:

MEZ	Frei wählbare Bezeichnung der Zeitzone; statt MEZ kann man z.B. auch Europa oder Hamburg eintragen
-1	Zeitdifferenz des Standortes zur Greenwich Zeit (für Hamburg -1 h)
M3.5.0	Beginn der Sommerzeit Mm.n.d (0[Sonntag]<=d<=6[Samstag], 1<=n<=5, 1<=m<=12) für den d. Tag von Woche n von Monat m des Jahres. Dabei ist Woche 1 die erste Woche, in der der Tag d vorkommt. Dabei steht ‚5’ für die letzte Woche, in der der Tag d vorkommt, das kann die 4. oder 5. Woche sein.

M10.5.0	Ende der Sommerzeit Mm.n.d (0[Sonntag]<=d<=6[Samstag], 1<=n<=5, 1<=m<=12) für den d. Tag von Woche n von Monat m des Jahres. Dabei ist Woche 1 die erste Woche, in der der Tag d vorkommt. Dabei steht ‚5' für die letzte Woche, in der der Tag d vorkommt, das kann die 4. oder 5. Woche sein.
/3	Uhrzeit, zu der die Sommerzeit endet : hier 3 Uhr morgens. Wenn kein Eintrag vorgenommen wird, wird der Zeitpunkt der Umstellung auf 2:00 Uhr gesetzt.

Zeitmarke im Dateisystem (2h Auflösung): Ja / Nein

Ist dieser Schalter auf *Ja* gesetzt, schreibt das MD740-1 alle 2 Stunden die aktuelle Systemzeit in seinen Speicher.

Folge: Wird das MD740-1 aus- und wieder eingeschaltet, wird nach dem Einschalten eine Uhrzeit in diesem 2-Stunden-Zeitfenster angezeigt und nicht eine Uhrzeit am 1. Januar 2000.

4.5.6 Dienste → Remote Logging

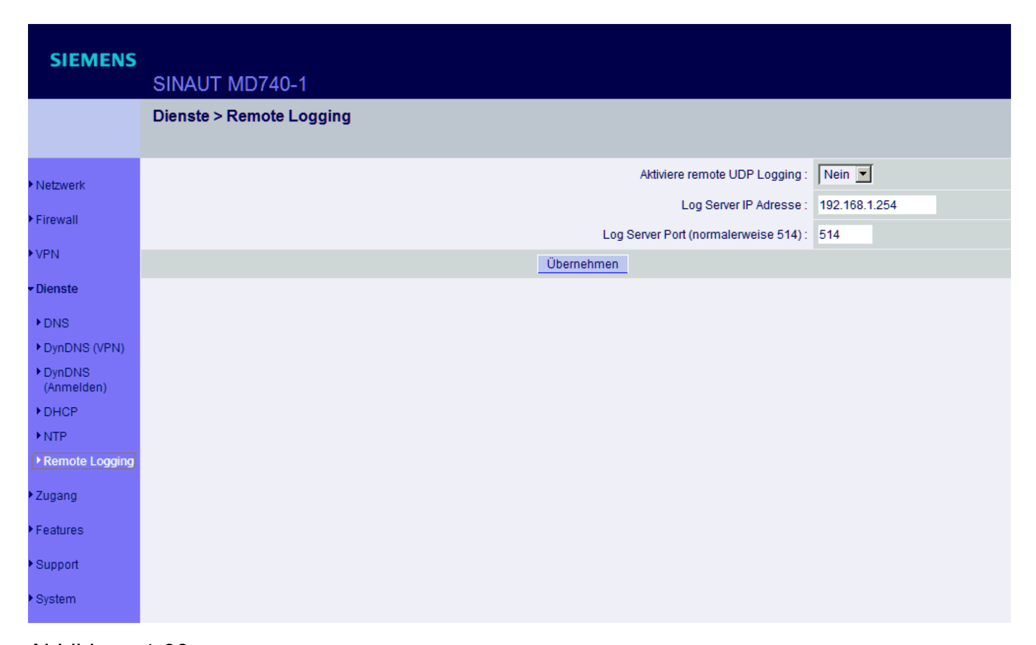


Abbildung 4-33

Alle Log-Einträge finden standardmäßig im Flashspeicher des MD740-1 statt. Ist der maximale Speicherplatz für diese Protokollierungen erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben.

Es ist möglich, die Log-Einträge auf einen externen Rechner zu übertragen. Das liegt z.B. dann nahe, soll eine zentrale Verwaltung der Protokollierungen erfolgen.

Hinweis

Ausgiebiges Loggen auf dem internen Flashspeicher des Gerätes kann die Lebensdauer des Gerätes verringern. Protokollieren Sie nur unbedingt notwendige Informationen.

Aktiviere remote UDP Logging: Ja / Nein

Sollen alle Log-Einträge zum externen (unten angegebenen) Log Server übertragen werden, setzen Sie diesen Schalter auf *Ja*.

Log Server IP-Adresse

Geben Sie die IP-Adresse des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen.

- Der Log-Server muss über eine feste und bekannte IP-Adresse verfügen!
- Sie müssen die IP-Adresse angeben, keinen Hostnamen! Hier wird eine Namensauflösung nicht unterstützt, weil sonst der Ausfall eines DNS-Servers nicht protokolliert werden könnte.

Log Server Port

Geben Sie den Port des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514

4.6 Menü-Zugang

4.6.1 Zugang → Passworte

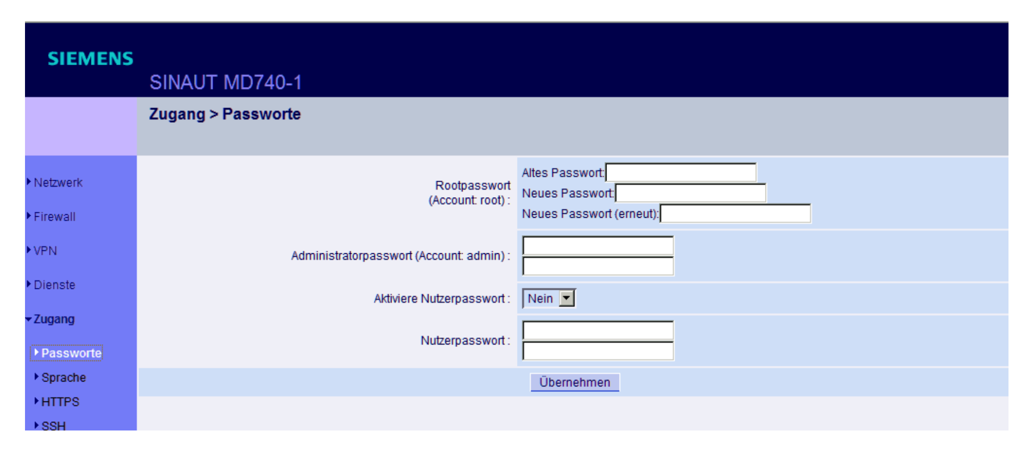


Abbildung 4-34

Das MD740-1 bietet 3 Stufen von Benutzerrechten. Höchste Berechtigungsstufe hat Root, gefolgt von Admin und dann Nutzer. Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, dass der jeweiligen Berechtigungsstufe zugeordnet ist.

Berechtigungsstufen

Root	Bietet erweiterte Rechte für die Parameter des MD 740-1 **Vorsicht:** Bei SSH-Zugang mit dieser Berechtigungsstufe ist es möglich, das Gerät so zu verkonfigurieren, dass es zum Service eingeschickt werden muss. Kontaktieren Sie in diesem Fall bitte Ihren Händler oder Distributor. Voreingestellter Benutzername: **root** Voreingestelltes Rootpasswort: **root** Der Benutzername **root** kann nicht geändert werden.
Administrator	Bietet die Rechte für alle Konfigurationsoptionen, die auch über die webbasierte Administratoroberfläche zugänglich sind. Voreingestellter Benutzername: **admin** Voreingestelltes Passwort: **sinaut** Der Benutzername **admin** kann nicht geändert werden.
Nutzer	Ist ein Nutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des MD740-1 bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, damit VPN-Verbindungen möglich sind. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest.

Tabelle 4-5

Rootpasswort

Werksseitig voreingestellt: **root**

Wollen Sie das Rootpasswort ändern, geben Sie in das Feld *Altes Passwort* das alte Passwort ein, in die beiden Felder darunter das neue, gewünschte Passwort. (unveränderbarer Benutzername: root)

Administratorpasswort (Account: admin)

Werksseitig voreingestellt: **sinaut**
(unveränderbarer Benutzername: admin)

Aktiviere Nutzerpasswort: Ja / Nein

Werksseitig ist Nutzerpasswortschutz ausgeschaltet.

Ist unten ein Nutzerpasswort festgelegt, kann der Nutzer-Passwortschutz mit diesem Schalter aktiviert bzw. deaktiviert werden.

Nutzerpasswort

Werksseitig ist kein Nutzerpasswort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

4.6.2 Zugang → Sprache



Abbildung 4-35

Bitte wählen Sie eine Sprache aus

Ist in der Sprachauswahlliste *(Automatisch)* ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Browser des Rechners.

4.6.3 Zugang → HTTPS



Abbildung 4-36

Bei eingeschaltetem HTTPS Fernzugang kann das MD740-1 über seine webbasierte Administratoroberfläche von einem entfernten Rechner aus konfiguriert werden. Das heißt, auf dem entfernten Rechner wird der Browser benutzt, um das lokale MD740-1 zu konfigurieren.

Standardmäßig ist diese Option ausgeschaltet.

Hinweis

Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt sind.

HTTPS Fernzugang

Um HTTPS Fernzugang zu ermöglichen, machen Sie nachfolgende Einstellungen:

Aktiviere HTTPS Fernzugang: Ja / Nein

Wollen Sie HTTPS Fernzugriff ermöglichen, setzen Sie diesen Schalter auf *Ja*.

Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln so zu setzen, dass von außen auf das MD740-1 zugegriffen werden kann.

Wenn Sie diesen Parameter per Fernzugriff auf *Nein* setzen, sind per HTTPS Fernzugriff keine weiteren Eingaben möglich. Diese Option muss dann wieder freigeschaltet werden, entweder lokal oder über SSH-Fernzugriff, sofern dieser konfiguriert ist.

Port für HTTPS-Verbindungen (nur Fernzugang)

Standard: 443

Sie können einen anderen Port festlegen.

Wenn Sie einen anderen Port festgelegt haben, dann muss die entfernte Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe hinter der IP-Adresse die Port-Nummer angeben.

Beispiel:
Ist dieses MD740-1 über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 442 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser angegeben werden:
192.144.112.5:442

Firewall-Regeln zu Freigabe des HTTPS-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines HTTP-Fernzugriffs.

Regel löschen:

- Klicken Sie neben dem betreffenden Eintrag *Löschen*.

Neue Regel setzen

1. Wollen Sie eine neue Regel setzen, klicken Sie *Neu*.
2. Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie *Übernehmen*.

Von IP

Geben Sie hier die Adresse(n) des/der Rechner(s) an, dem/denen Fernzugang erlaubt ist. Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse oder -Adressenbereich: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 4.10.

Interface

extern (fest vorgegeben)

Aktion

Möglichkeiten: *Annehmen / Abweisen / Verwerfen*

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen oder nicht - *Log* auf *Nein* setzen (werksseitige Voreinstellung).

4.6.4 Zugang → SSH



Abbildung 4-37

Bei eingeschaltetem SSH Fernzugang kann das MD740-1 von einem entfernten Rechner aus konfiguriert werden. Dazu muss zunächst mit einem SSH-fähigen Programm eine Verbindung von der entfernten Station zum MD740-1 aufgebaut werden. Einstellungen im MD740-1 nehmen Sie über die SSH-Console mit dem Kommando „gaiconfig“ vor.

Standardmäßig ist diese Option ausgeschaltet.

Hinweis

Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt sind.

Vorsicht

Bei SSH-Zugang über das Root-Passwort ist es möglich, das Gerät so zu verkonfigurieren, dass es zum Service eingeschickt werden muss. Kontaktieren Sie in diesem Fall bitte Ihren Händler oder Distributor.

SSH Fernzugang

Um SSH Fernzugang zu ermöglichen, machen Sie folgende Einstellungen:

Aktiviere SSH Fernzugang: Ja / Nein

Wollen Sie SSH Fernzugriff ermöglichen, setzen Sie diesen Schalter auf *Ja*.

Hinweis

Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln so zu setzen, dass von außen auf das MD740-1 zugegriffen werden kann.

Port für SSH-Verbindungen (nur Fernzugang)

Standard: 22

Anderer Port:
Sie können einen anderen Port festlegen. Wenn Sie einen anderen Port festgelegt haben, dann muss die entfernte Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe vor der IP-Adresse die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:
Ist dieses MD740-1 über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang eine andere Port-Nummer festgelegt, dann muss bei der entfernten Gegenstelle im SSH-Client (z. B. Web-Browser) diese Port-Nummer angegeben werden, z.B.

ssh -p 22222 192.144.112.5

Firewall-Regeln zu Freigabe des SSH-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SSH-Fernzugriffs.

Regel löschen

Klicken Sie neben dem betreffenden Eintrag *Löschen*.

Neue Regel setzen

Wollen Sie eine neue Regel setzen, klicken Sie *Neu*.

Legen Sie die gewünschte Regel fest (s. u.) und klicken Sie *Übernehmen*.

Von IP

Geben Sie hier die Adresse(n) des/der Rechner(s) an, dem/denen Fernzugang erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 4.10.

Interface

extern (fest vorgegeben)

Aktion

Möglichkeiten: *Annehmen / Abweisen / Verwerfen*

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
oder nicht - *Log* auf *Nein* setzen (werksseitige Voreinstellung).

4.7 Menü Features

4.7.1 Features → Installiere Update

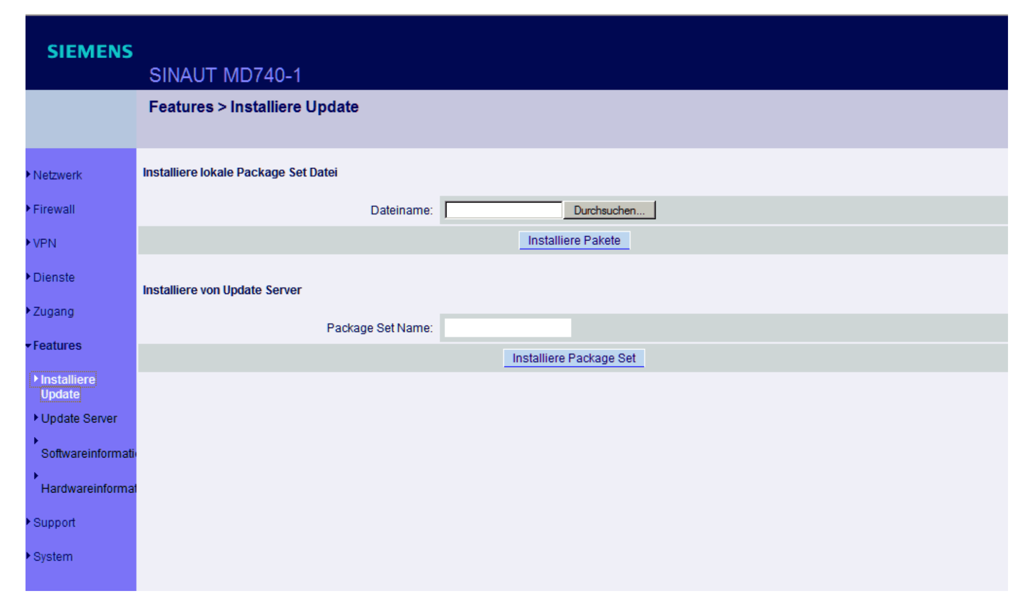


Abbildung 4-38

Voraussetzung

Sie haben ein aktuelles Software-Paket entweder lokal auf Ihrem Konfigurations-Rechner gespeichert oder über einen entfernten Server zur Verfügung gestellt bekommen.

Software Updates erhalten Sie über Service & Support im Internet. Weitere Informationen enthält Seite 7.

Achtung

Sie dürfen während des Updates auf keinen Fall die Stromversorgung des MD740-1 unterbrechen! Das Gerät könnte ansonsten beschädigt und nur noch durch den Hersteller reaktiviert werden

---

Haben Sie ein aktuelles Software-Update auf Ihrem Konfigurations-Rechner gespeichert, gehen Sie wie folgt vor:

1. *Durchsuchen...* klicken und dann die Datei selektieren.
2. *Installiere Pakete* klicken, um sie in das Gerät zu laden.

Dieser Vorgang kann je nach Größe des Updates mehrere Minuten dauern.

Sollte nach dem System-Update ein Reboot erforderlich sein, wird dies angezeigt.

Wird Ihnen ein aktuelles Software-Update auf einem entfernten Server zur Verfügung gestellt, muss dessen Adresse festgelegt sein - siehe Kapitel 4.7.2.

Gehen Sie wie folgt vor:

1. Schreiben Sie den Dateinamen in das Eingabefeld.
2. *Installiere Package Set* klicken, um sie in das Gerät zu laden.

Dieser Vorgang kann je nach Größe des Updates mehrere Minuten dauern.

Sollte nach dem System-Update ein Reboot erforderlich sein, wird dies angezeigt.

4.7.2 Features → Update Server

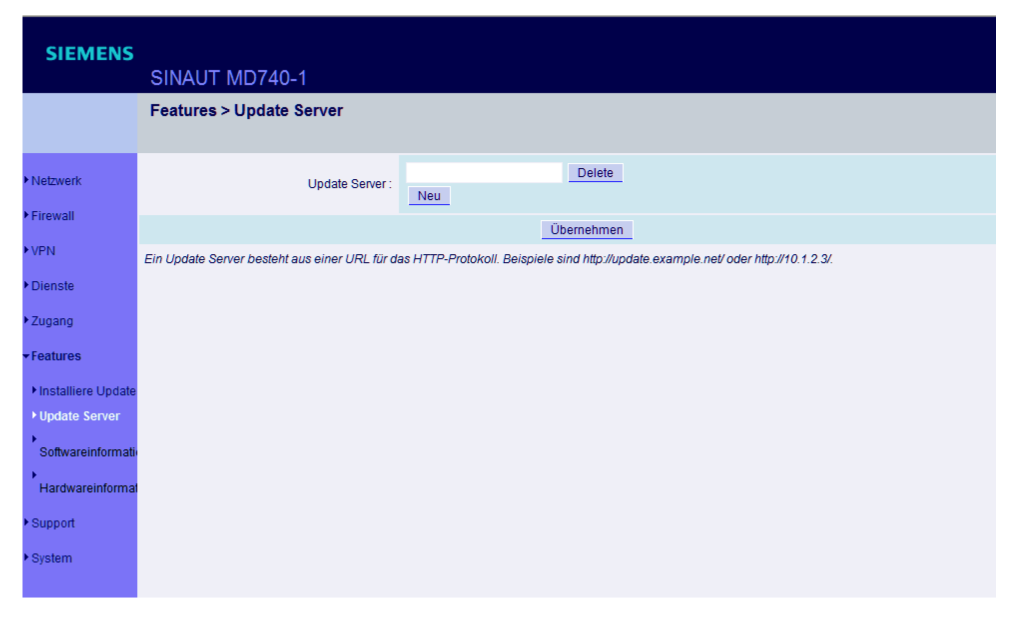
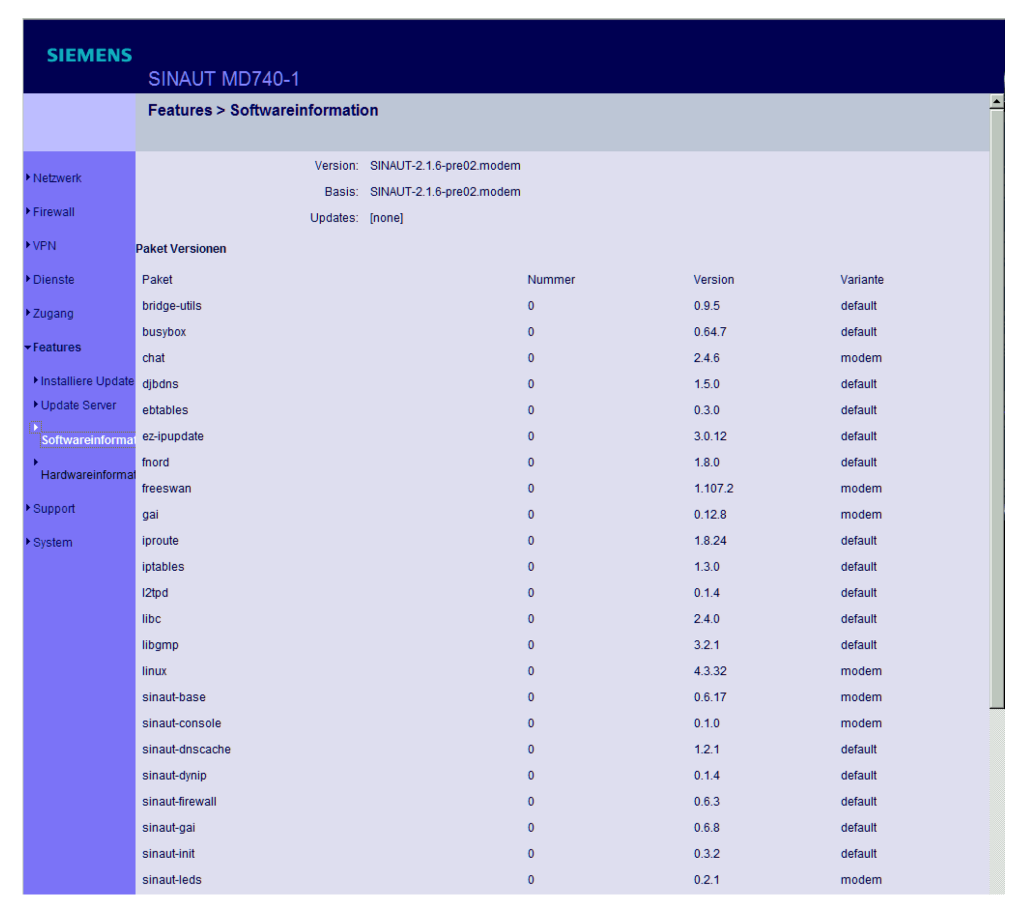


Abbildung 4-39

Wird Ihnen ein Software-Update (*Features → Installiere Update*) des MD740-1 auf einem entfernten Server zur Verfügung gestellt, dann geben Sie hier dessen Adresse an. Dieser muss auf jeden Fall das benutzte Protokoll, z. B. http, voran stehen.

Beispiele: http://123.456.789.1 ODER http://www.xyz.com/update

4.7.3 Features → Softwareinformationen



Paket	Nummer	Version	Variante
bridge-utils	0	0.9.5	default
busybox	0	0.64.7	default
chat	0	2.4.6	modem
djbdns	0	1.5.0	default
ebtables	0	0.3.0	default
ez-ipupdate	0	3.0.12	default
fnord	0	1.8.0	default
freeswan	0	1.107.2	modem
gai	0	0.12.8	modem
iproute	0	1.8.24	default
iptables	0	1.3.0	default
l2tpd	0	0.1.4	default
libc	0	2.4.0	default
libgmp	0	3.2.1	default
linux	0	4.3.32	modem
sinaut-base	0	0.6.17	modem
sinaut-console	0	0.1.0	modem
sinaut-dnscache	0	1.2.1	default
sinaut-dynip	0	0.1.4	default
sinaut-firewall	0	0.6.3	default
sinaut-gai	0	0.6.8	default
sinaut-init	0	0.3.2	default
sinaut-leds	0	0.2.1	modem

Abbildung 4-40

Nur Anzeige:

Listet die im Gerät befindlichen Software-Module auf. Diese werden als Pakete bezeichnet.

Dient für Update-Zwecke: Vergleichen Sie die angezeigten Versionsnummern mit den aktuellen Versionsnummern der entsprechenden Pakete. Bitte wenden Sie sich dazu an Ihren Distributor.

Falls neue Versionen verfügbar sind, können Sie die Software im Gerät updaten. Siehe Kapitel 4.7.2.

4.7.4 Features → Hardwareinformationen

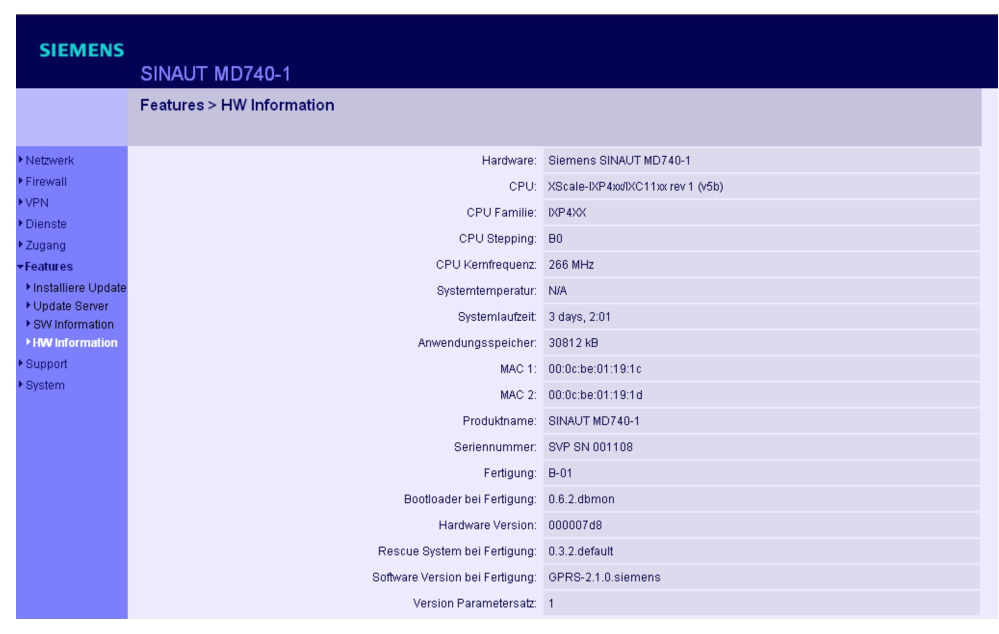


Abbildung 4-41

Aufgelistet werden Hardware-nahe Kenndaten des Router-Teils. Eventuell werden Sie bei Anfragen an den Support nach einigen dieser Kenndaten gefragt.

4.8 Menü Support

4.8.1 Support → Snapshot



Abbildung 4-42

Diese Funktion dient für Support-Zwecke.

Erstellt eine komprimierte Datei (im tar-Format), in der alle aktuellen Konfigurations-Einstellungen und Log-Einträge erfasst sind, die zur Fehlerdiagnose relevant sein könnten.

Hinweis

Diese Datei enthält keine privaten Informationen wie z. B. das private Maschinen-Zertifikat oder die Passwörter. Eventuell benutzte Pre-Shared Keys von VPN-Verbindungen sind jedoch in den Snapshots enthalten.

Um einen Snapshot zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie *Herunterladen*.
2. Speichern Sie die Datei unter dem Namen *snapshot.tar.gz*

Stellen Sie die Datei dem Support zur Verfügung, wenn dies erforderlich ist.

4.8.2 Support → Status

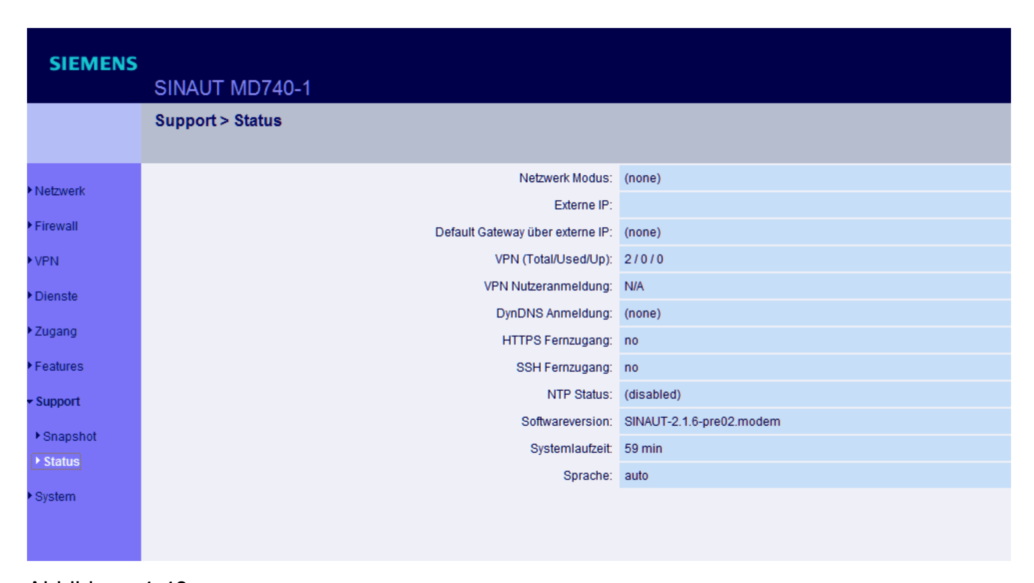


Abbildung 4-43

Nur Anzeige:

Zeigt eine Zusammenfassung verschiedener Statusinformationen für Support-Zwecke:

Netzwerk-Modus

Betriebsart des MD740-1: *modem*

Externe IP

Die IP-Adresse des MD740-1 an seinem Anschluss für das externe Netz (WAN bzw. Internet).

Default Gateway über externe IP

Hier wird die externe IP-Adresse des MD740-1 angezeigt.

VPN (Total / Used / Up)
Möglichkeiten: *Total / Used / Up*

Total : Insgesamt eingerichtete VPN-Verbindungen

Used : Benutzte VPN-Verbindungen

Up : Gegenwärtig aktive VPN-Verbindungen

VPN Nutzeranmeldung
Möglichkeiten:

N / A : Nicht verfügbar (not available)

not logged in : VPN gesperrt

logged in : VPN freigeschaltet

DynDNS Anmeldung
Möglichkeiten:

none / Angabe des DynDNS-Server / failure / trying

none :
Kein DynDNS-Server angegeben

Angabe des DynDNS-Server :
Adresse des DynDNS-Servers, den das MD740-1 zur Auflösung von Hostnamen benutzt

failure :
Das MD740-1 versucht vergeblich, eine Verbindung zum DynDNS-Server herzustellen.

trying :
Das MD740-1 versucht gerade, eine Verbindung zum DynDNS-Server herzustellen.

HTTPS Fernzugang
Möglichkeiten: *no / yes*

SSH Fernzugang
Möglichkeiten: *no / yes*

NTP Status
Möglichkeiten: *synchonized / not synchronized*

synchronized :
Über das Network Time Protokoll empfängt das MD740-1 von einem Zeitserver die aktuelle Uhrzeit (Greenwich-Zeit).

not synchronized :
Das MD740-1 ist mit keinem Zeitserver verbunden und kann deshalb nicht die aktuelle Uhrzeit liefern.

Softwareversion

Version der im MD740-1 installierten Software

Systemlaufzeit

Laufzeit seit dem letzten Startvorgang des MD740-1

Sprache

Aktuell eingestellte Sprache

4.9 Menü System

4.9.1 System → Konfigurations-Profile

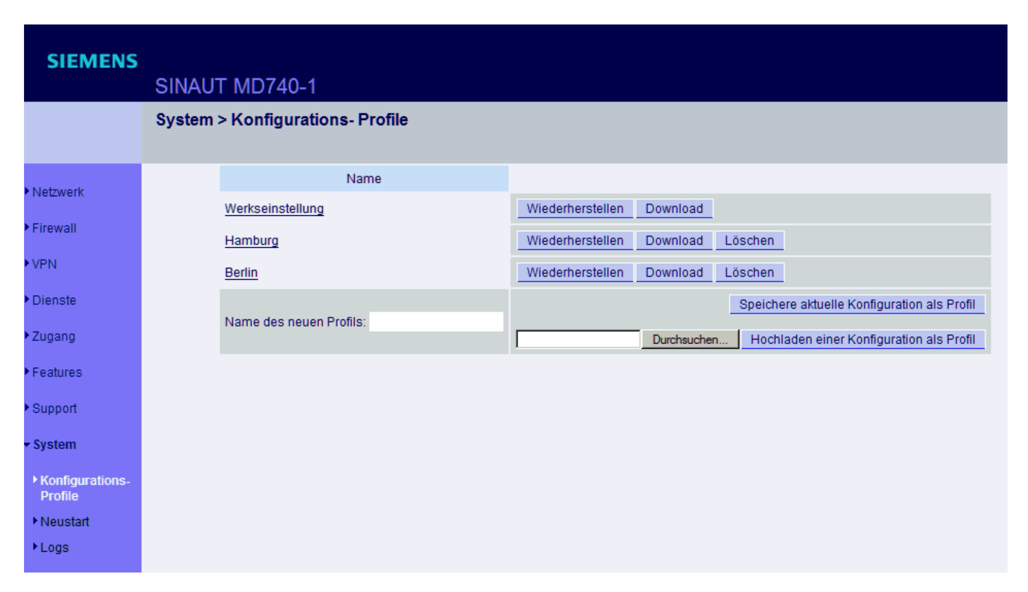


Abbildung 4-44

Sie haben die Möglichkeit, die Einstellungen des MD740-1 als Konfigurations-Profil unter einem beliebigen Namen im MD740-1 zu speichern. Sie können mehrere solcher Konfigurations-Profile anlegen. Dann können Sie bei Bedarf mal das eine, mal das andere Konfigurations-Profil aktivieren, wenn Sie das MD740-1 in unterschiedlichen Betriebsumgebungen einsetzen.

Darüber hinaus können Sie Konfigurations-Profile als Dateien auf der Festplatte des Konfigurations-Rechners abspeichern. Umgekehrt besteht die Möglichkeit, eine so erzeugte Konfigurationsdatei in das MD740-1 zu laden und in Kraft zu setzen.

Zusätzlich haben Sie die Möglichkeit, jederzeit die Werkseinstellung (wieder) in Kraft zu setzen.

Hinweis

Beim Abspeichern eines Konfigurations-Profils werden Passwörter und Benutzernamen nicht mitgespeichert.

Aktuelle Konfiguration als Konfigurations-Profil speichern

Wenn Sie die aktuelle Konfiguration als Konfigurations-Profil im MD740-1 speichern wollen, gehen Sie wie folgt vor:

1. In Feld *Name des neuen Profils* den gewünschten Namen eintragen
2. Die Schaltfläche *Speichere aktuelle Konfiguration als Profil* klicken.

Ein im MD740-1 gespeichertes Konfigurations-Profil anzeigen /aktivieren / löschen

Voraussetzung:
Es ist mindestens ein Konfigurations-Profil angelegt und im MD740-1 gespeichert.

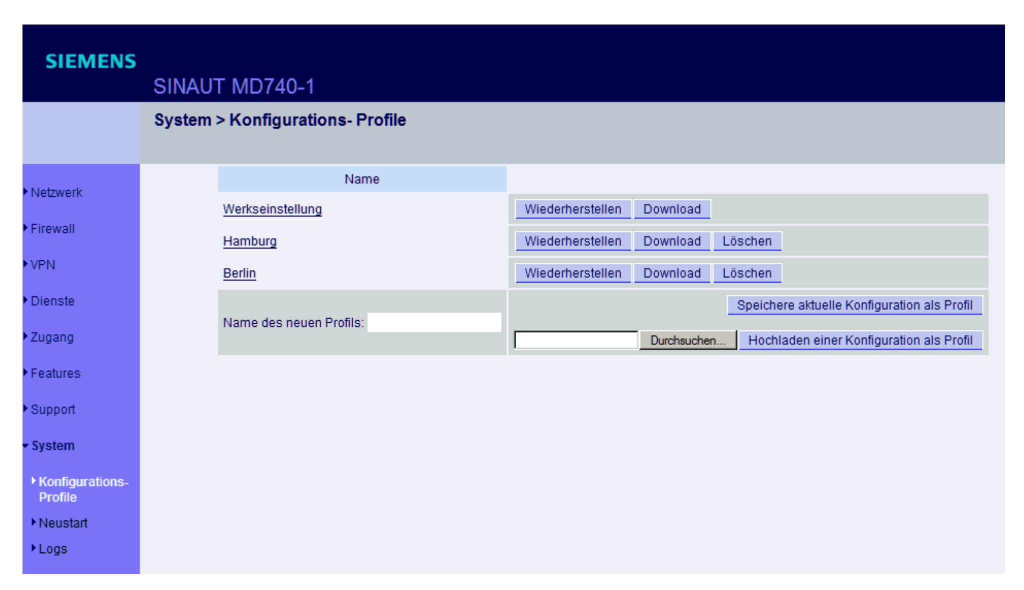


Abbildung 4-45 Angelegte Konfigurations-Profile (Beispiele)

Konfigurations-Profil anzeigen
Den Namen des Konfigurations-Profils anklicken.

Konfigurations-Profil aktivieren
Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche *Wiederherstellen* klicken.

Konfigurations-Profil löschen
Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche *Löschen* klicken.

Werkseinstellung anzeigen / aktivieren
Die Werkseinstellung ist als Konfigurations-Profil unter dem Namen *Werkseinstellung* im MD740-1 gespeichert.

Anzeigen: Den Namen *Werkseinstellung* anklicken.

Aktivieren: Neben dem Namen *Werkseinstellung* die Schaltfläche *Wiederherstellen* klicken.

Hinweis

Es ist nicht möglich, das Konfigurations-Profil *Werkseinstellung* zu löschen

Konfigurations-Profil als Datei auf Festplatte speichern

Zum Speichern des Konfigurations-Profil als Datei auf der Festplatte gehen Sie wie folgt vor:

1. Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche *Download* klicken.
2. Legen Sie im angezeigten Dialogfeld den Dateinamen und Ordner fest, unter bzw. in dem das Konfigurations-Profil als Datei gespeichert wird. (Sie können die Datei beliebig benennen.)

Konfigurations-Profil von Festplatte in das MD740-1 laden

Voraussetzung:

Sie haben nach dem oben beschriebenen Verfahren ein Konfigurations-Profil als Datei auf der Festplatte des Konfigurations-Rechners gespeichert.

Dann wie folgt vorgehen:

1. In Feld *Name des neuen Profils* den Namen eintragen, den das einzuladende Konfigurations-Profil erhalten soll.
2. Die Schaltfläche *Durchsuchen* klicken und dann die Datei selektieren.
3. Die Schaltfläche *Hochladen einer Konfiguration als Profil* klicken.

Folge: Die hochgeladene Konfiguration erscheint in der Liste der Konfigurations-Profile.

Soll das hochgeladene Konfigurations-Profil aktiviert werden, klicken Sie neben dem Namen auf *Wiederherstellen*.

4.9.2 System → Neustart



Abbildung 4-46

Ein Neustart (= Reboot) ist gegebenenfalls im Fehlerfall oder nach einem Software-Update erforderlich.

Am Ende des Neustarts erscheint der Text „Neu gestartet“.

Ein Reboot kann auch durch Aus- und wieder Einschalten des Gerätes bewirkt werden.

4.9.3 System → Logs

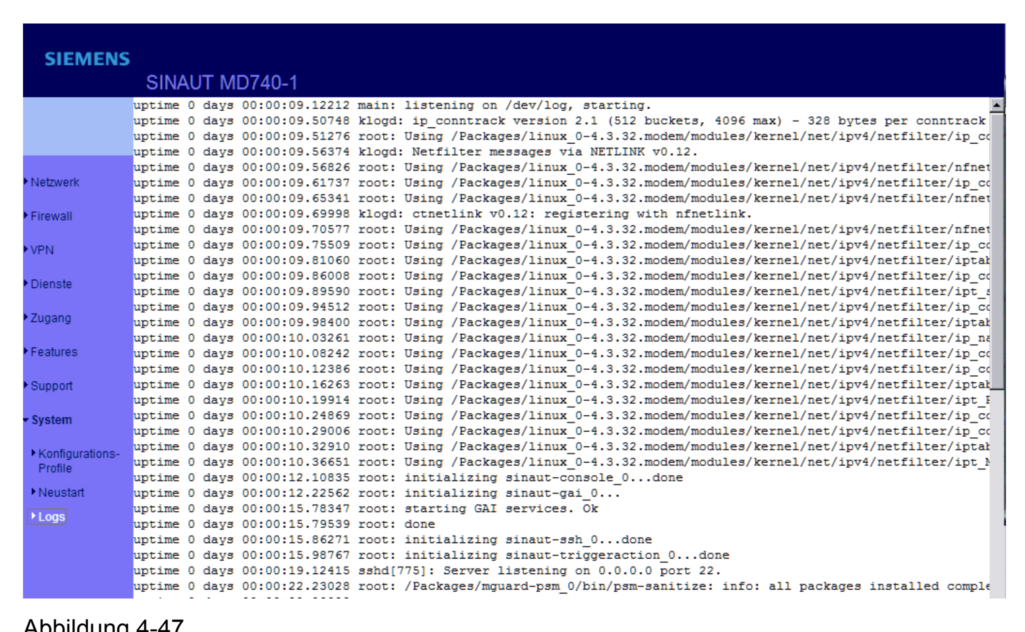


Abbildung 4-47

Zeigt alle aufgezeichneten Log-Einträge (Gesamtlog).

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

Sie können die Log-Einträge auf einen externen Server übertragen. Siehe Kapitel 4.5.6.

Hinweis

Nach einem Neustart des Gerätes werden bereits Einträge im Log-File vorgenommen, bevor das Gerät die Systemzeit synchronisieren kann. In diesem Fall sind die Zeitstempel nicht chronologisch angeordnet. Die Reihenfolge der Einträge ist jedoch chronologisch.

4.10 CIDR (Classless InterDomain Routing)

IP-Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinander folgenden Adressen als ein Netzwerk behandelt.

Das CIDR-Verfahren reduziert die z. B. in Routern gespeicherten Routing-Tabellen durch ein Postfix in der IP-Adresse. Mit diesem Postfix können ein Netz und die darunter liegenden Netze zusammengefasst bezeichnet werden. Die Methode ist in RFC 1518 beschrieben.

Um dem MD740-1 einen Bereich von IP-Adressen anzugeben z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

4.11 Netzwerkbeispiele

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.

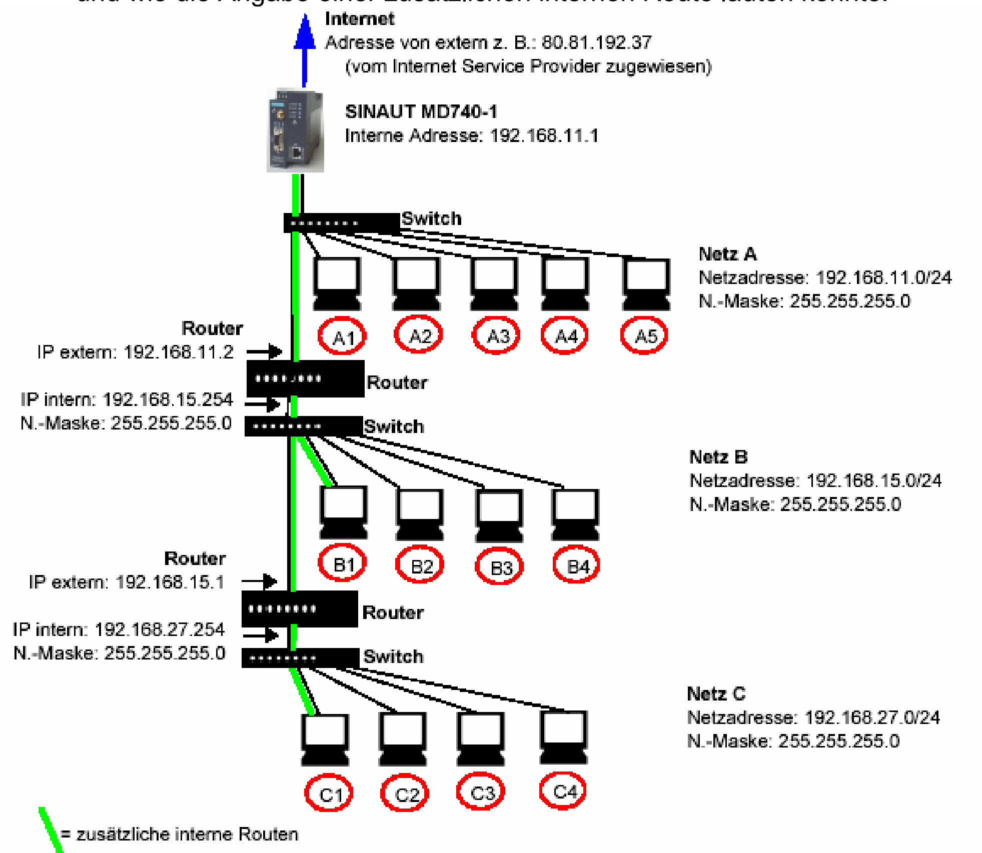


Abbildung 4-48

Netz A					
Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Netz B					
Rechner	B1	B2	B3	B4	**Zusätzliche interne Routen:** Netzwerk: 192.168.15.0/24 Gateway: 192.168.11.2 Netzwerk: 192.168.27.0/24 Gateway: 192.168.11.2
IP-Adresse	192.168.15.3	192.168.15.4	192.168.15.5	192.168.15.6	
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Netz C					
Rechner	C1	C2	C3	C4	
IP-Adresse	192.168.27.3	192.168.27.4	192.168.27.5	192.168.27.6	
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	

Netz A ist an das SINAUT MD740-1 angeschlossen und über dieses mit einem entfernten Netz verbunden. Zusätzliche interne Routen zeigen den Weg zu

weiteren Netzen (Netz B, C), die über Gateways (Router) miteinander verbunden sind. Für das MD740-1 sind bei dem gezeigten Beispiel die Netze B und C beide über das Gateway 192.168.11.2 und der Netzwerkadresse 192.168.11.0/24 erreichbar.

Integrierte Website zeigt Geräte- und Verbindungsdaten des Modem-Teils 5

Einleitung

Das SINAUT MD740-1 setzt sich aus zwei weitgehend unabhängigen Komponenten zusammen, dem Router-Teil mit den Firewall- und VPN-Funktionen sowie dem Modem-Teil für die Kommunikation über GPRS. Beide Teile verfügen jeweils über einen eigenen Web-Server zur Konfiguration und zur Anzeige von Geräte- und Verbindungsdaten. Die Konfigurations- und Anzeigemöglichkeiten über den Web-Server des Router-Teils sind im Kapitel 4 beschrieben. Der Web-Server des Modem-Teils stellt eine Website bereit, die über Geräte- und Verbindungsdaten informiert. In diesem Kapitel geht es um die Website des GPRS-Moduls, nicht um die des VPN-Routers.

Es gibt verschiedene Möglichkeiten, auf die Website mit Hilfe eines Web-Browsers zuzugreifen:

- lokal über die Service-Schnittstelle - siehe Kapitel 5.1
- lokal über die Applikations-Schnittstelle (Buchse 10/100 BASE-T) - siehe Kapitel 5.2
- von einem entfernten Rechner aus über das GPRS-Netz (netzabhängig) – siehe Kapitel 5.3.

5.1 Lokal über die Service-Schnittstelle auf den Web-Server des Modem-Teils zugreifen

Per DFÜ-Verbindung

Um das MD740-1 über seine Service-Schnittstelle anzusprechen, müssen folgende Bedingungen erfüllt sein:

- Der Rechner, den Sie dazu benutzen wollen, muss über einen seiner COM-Ports an der Service-Schnittstelle des MD740-1 angeschlossen sein.
- Auf diesem Rechner muss eine entsprechende DFÜ-Verbindung eingerichtet sein (s.u.). Diese muss folgende Daten enthalten:
  - die Einwahl-Zeichenkette für die Einwahl in die Service-Schnittstelle: ***98#**
  - Benutzername und Passwort: jeweils **service**
  - Modem bzw. Gerät, über das die Verbindung hergestellt werden soll: Standard Modem 19200. Die Modemtreiberdatei muss zuvor installiert worden sein (s. u.).

Modem für Zugriff auf die Serviceschnittstelle installieren

Zur Installation des Modemtreibers gehen Sie bei Windows XP wie folgt vor. Die Installation unter Windows 2000 erfolgt entsprechend.

Hinweis

Bei Verwendung von Windows 2000 oder XP müssen Sie als Administrator angemeldet sein. Achten Sie in diesen Fällen bitte darauf, dass für die ausgewählte Schnittstelle keine weiteren Modemtreiber installiert sind oder werden.

---

1. Klicken Sie *Start, Systemsteuerung*, so dass das Dialogfeld *Systemsteuerung* erscheint.
2. Schalten Sie auf "klassische Ansicht".
3. Das Symbol *Telefon- und Modemoptionen* doppelklicken.
4. Im Dialogfeld *Telefon- und Modemoptionen* auf der Registerkarte *Modems* die Schaltfläche *Hinzufügen...* klicken.
5. Der Hardware-Assistent zur Installation eines neuen Modems erscheint. Folgen Sie den Anweisungen des Hardware-Assistenten:

Hinweis

Legen Sie fest, dass Sie selbst das Modem auswählen, also keine automatische Erkennung stattfindet.

Bei der Auswahl des Modems wählen Sie folgendes Modell:
Standard 19200 bps Modem

DFÜ-Verbindung für die Service-Schnittstelle einrichten

Zur Einrichtung der DFÜ-Verbindung für die Service-Schnittstelle gehen Sie wie folgt vor:

Windows 2000:

1. Klicken Sie *Start - Einstellungen - Netzwerk- und DFÜ-Verbindungen - Neue Verbindung erstellen*, so dass der Netzwerkverbindungs-Assistent gestartet wird.

2. Wählen Sie: *In das Internet einwählen, Manuelle Einrichtung der Internetverbindung..., Verbindung über Telefonleitung und Modem*.

Folgen Sie den Anweisungen in den Dialogfeldern.

Hinweis

Achten Sie darauf, dass keine Orts- oder Wählparameter verwendet werden.

Windows XP:

1. Klicken Sie *Start - Systemsteuerung*: In der klassischen Ansicht *Netzwerkverbindungen doppelklicken,* dann *Neue Verbindung erstellen* klicken, so dass der *Assistent für neue Verbindungen* gestartet wird.

2. Wählen Sie: *Verbindung mit dem Internet herstellen, Verbindung manuell einrichten, Verbindung mit einem DFÜ-Modem herstellen.*

Folgen Sie den Anweisungen in den Dialogfeldern.

Hinweis

Achten Sie darauf, dass keine Orts- oder Wählparameter verwendet werden.

Verbindung zur Website des MD740-1 herstellen

1. Doppelklicken Sie das Symbol der DFÜ-Verbindung, die für die CSD-Einwahl eingerichtet ist.

   Das Dialogfeld *Verbindung ... herstellen* erscheint. Benutzername und Passwort lauten jeweils: **service**

2. Klicken Sie *Wählen*.

   Wirkung:
   Der Rechner ist mit dem MD740-1 in der Weise verbunden, dass der integrierte Web-Server angesprochen werden kann.

3. Starten Sie Ihren Web-Browser, z. B. den MS Internet Explorer.
   In der Adresszeile des Browsers geben Sie die Adresse der internen Website ein. Diese lautet:

   http://192.168.0.8

   Wirkung:
   Die Startseite der im MD740-1 gespeicherten Website wird angezeigt - siehe Kapitel 5.4.

4. Klicken Sie die Hyperlinks der gewünschten HTML-Seiten, um diese einzusehen.

5. Trennen Sie abschließend die DFÜ-Verbindung.

Service-Verbindung trennen

Unten rechts auf dem Bildschirm im Info-Bereich das Verbindungssymbol mit der rechten Maustaste anklicken und im geöffneten Menü *Verbindung Trennen* klicken.

5.2 Lokal über die Applikations-Schnittstelle (Buchse 10/100 BASE-T) auf den Web-Server des Modem-Teils zugreifen

Auf den internen WEB-Server des Modem-Moduls kann zur Ansicht der Geräte- und Verbindungsdaten auch von der Ethernet-Schnittstelle des VPN-Routers zugegriffen werden.

Voraussetzungen

Das SINAUT MD740-1 setzt sich aus zwei weitgehend unabhängigen Komponenten zusammen, dem Router-Teil mit den Firewall- und VPN-Funktionen und dem Modem-Teil für die Kommunikation über GPRS. Beide Teile kommunizieren über eine PPP-Verbindung miteinander, die nur dann besteht, wenn auch eine GPRS-Verbindung aufgebaut ist. Daher kann die am Router-Teil angeschlossene Applikation sich nur bei bestehender GPRS-Verbindung mit der Web-Site des Modem-Teils verbinden.

Zwischen dem Router-Teil und dem Modem-Teil liegt außerdem die Firewall, die die angeschlossene Applikation vor Zugriffen von außen schützt. Für Zugriffe auf die Web-Site des Modem-Teils muss daher eine Firewall-Regel definiert werden.

Darum gelten folgende Voraussetzungen:

- Es muss eine GPRS-Verbindung bestehen. D. h. die C-LED des MD740-1 leuchtet und signalisiert, dass vom GPRS-Netz eine IP-Adresse zugewiesen ist.
- Bei der Adresse des lokal angeschlossenen Rechners, der auf die interne Website zugreifen soll, muss NAT stattfinden (siehe Kapitel 4.3.4).
- Die Firewall des MD740-1 muss die Datenpakete passieren lassen, die der lokal angeschlossene Rechner zum Web-Server des MD740-1 sendet (siehe Kapitel 4.3.2)

Beispiel:
Soll der Rechner, den Sie auch zur Konfiguration des MD740-1 benutzen (eigene Adresse 192.168.1.2), Zugriff auf die im MD740-1 gespeicherte Website haben, lauten die Einstellungen beispielsweise wie folgt:

Einstellung Firewall → NAT:

Mögliche Adressen-Angaben: 192.168.1.2 oder 192.168.1.0/24

Einstellung Firewall → Ausgehend:

Prot.	*Von IP*	*Von Port*	*Nach IP*	*Nach Port*	*Aktion*
TCP	192.168.1.2	any	192.168.0.8	any	Annehmen
ODER					
TCP	192.168.1.0/24	any	192.168.0.8	any	Annehmen

Verbindung zur Website des Modem-Teils des MD740-1 herstellen

1. Starten Sie Ihren Web-Browser, z. B. den MS Internet Explorer.

   In der Adresszeile des Browsers geben Sie die Adresse der internen Website ein. Diese lautet: http://192.168.0.8

   Wirkung:

   Die Startseite der im MD740-1 gespeicherten Website wird angezeigt - siehe Kapitel 5.4.

2. Klicken Sie die Hyperlinks der gewünschten HTML-Seiten, um diese einzusehen.

5.3 Von einem entfernten Rechner aus über das GPRS-Netz auf den Web-Server des Modem-Teils des MD740-1 zugreifen

Voraussetzung

- Die Zugriffsmöglichkeit ist abhängig von der Konfiguration des GPRS-Netzes und davon, wie Ihr LAN an das GPRS angebunden ist.
- Es muss eine GPRS-Verbindung zum entfernten MD740-1 bestehen. D. h. beim entfernten MD740-1 leuchtet die C-LED und signalisiert, dass vom GPRS-Netz eine IP-Adresse zugewiesen ist.

Verbindung zur Website des MD740-1 herstellen

1. Starten Sie Ihren Web-Browser, z. B. den MS Internet Explorer.

   In der Adresszeile des Browsers geben Sie die externe Adresse des MD740-1 an.

   Wirkung:

   Die Seite mit den Geräteinformationen wird angezeigt - siehe Kapitel 5.4.

2. Klicken Sie die Hyperlinks der gewünschten HTML-Seiten, um diese einzusehen.

5.4 Die Website des MD740-1

Um die Website des MD740-1 mit einem Web-Browser einsehen zu können, müssen die entsprechenden vorbereitenden Maßnahmen getroffen worden sein, je nach dem, ob Sie

- lokal über die Service-Schnittstelle
- lokal über die Applikations-Schnittstelle (Buchse 10/100 BASE-T) oder
- von einem entfernten Rechner aus über das GPRS-Netz (netzabhängig)

mit Ihrem Web-Browser auf die Website zugreifen wollen.

Sobald Sie im Web-Browser die Adresse **http://192.168.0.8** (bzw. die externe IP-Adresse des Gerätes, wenn Sie von einem entfernten Rechner auf die Web-Seiten zugreifen, siehe Abschnitt 5.3) eingegeben haben, erscheint die Seite *Device Information* der Website des MD740-1.

Durch Klicken auf den betreffenden Hyperlink können Sie sich die entsprechende HTML-Seite im Browser anzeigen lassen.

Seite *Device Information*

Klicken Sie auf der Startseite den Hyperlink *Device Information*, wenn Sie diese Seite einsehen wollen.

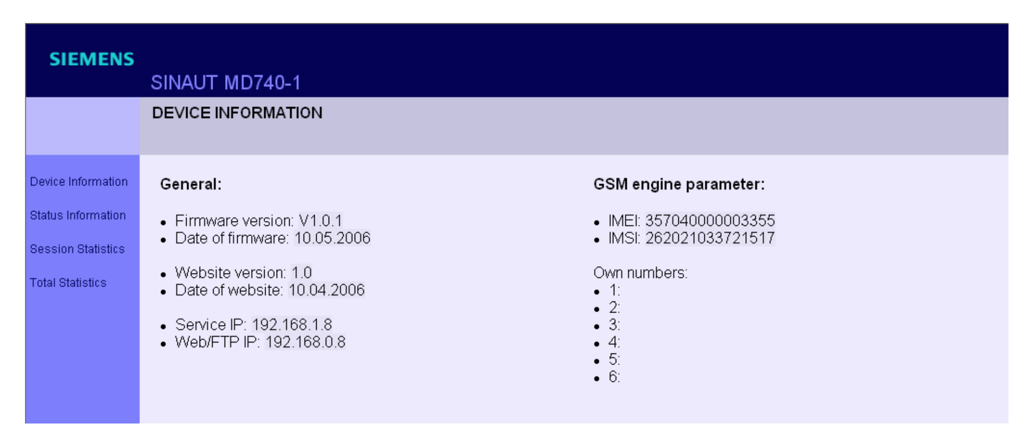


Abbildung 5-1

Erläuterungen

Firmware-Version:	Version der aktuell im Gerät vorhandenen Firmware
Date of Firmware:	Datum der letzten Firmware-Aktualisierung
Website Version:	Version der im Gerät vorhandenen HTML-Dateien
Date of Website:	Erstelldatum der HTML-Seiten
Service-IP:	IP-Adresse der Service-Schnittstelle
Web/FTP-IP:	IP-Adresse des internen **Web** und **FTP**-Servers

GSM Modul Daten

IMEI:	**I**nternational **M**obile station **E**quipment **I**dentity. Einmaliger unveränderlicher CODE, der dem internen Mobile (Handy)-Modul zugeordnet ist (Gerätenummer).
IMSI:	**I**nternational **M**obile **S**ubscriber **I**dentity (Internationale Kennungen für Mobile Teilnehmer). Die IMSI dient gemäß der Internationalen Fernmeldeunion (ITU) der international eindeutigen Identifikation von Teilnehmern in drahtlosen und drahtgebundenen Kommunikationsdiensten. Bei Mobiltelefonen ist die IMSI auf der SIM-Karte gespeichert.
Own numbers: (1..6):	Die auf der SIM-Karte gespeicherten (eigenen) Telefon-Nummern. Es werden die Voice, Data und Fax Nummern angezeigt, falls vorhanden.

Seiten Session Statistics und Total Statistics

Klicken Sie auf der Startseite den Hyperlink *Session Statistics* oder *Total Statistics*, wenn Sie diese Seiten einsehen wollen.
Geben Sie dann im Browser den Befehl *Aktualisieren*, damit die aktuellen Daten geladen werden.

PPP-Schicht (PPP - Point-to-Point-Protocol)

Links werden jeweils Informationen zur PPP-Schicht, rechts zur IP-Schicht gezeigt.



Abbildung 5-2: *Session Statistics* (links) und *Total Statistics* (rechts)

PPP Layer: Erläuterungen

Packets (Pakete):	
Received*:*	Anzahl der empfangenen PPP-Frames (Daten-Pakete)
Sent*:*	Anzahl der gesendeten PPP-Frames
Total*:*	Summe aller gesendeten und empfangenen PPP-Pakete während der Online-Verbindung
Invalid:	Anzahl der fehlerhaften (ungültigen) PPP-Frames
Bytes:	
Received:	Anzahl der empfangenen Daten-Bytes innerhalb eines PPP-Frames
Sent:	Anzahl der gesendeten Bytes eines PPP-Frames
Total:	Summe aller gesendeten und empfangenen Bytes auf PPP-Ebene
Invalid:	Anzahl der fehlerhaften Bytes
Online time:	Gibt an, wie lange die aktuelle GPRS-Verbindung besteht. Anzeige in „*Stunden.Minuten.Sekunden*“.

IP-Schicht (IP - Internet Protocol)

IP Layer: Erläuterungen

Packets (Pakete):	
Received:	Anzahl der empfangenen IP-Frames
Sent:	Anzahl der gesendeten IP-Frames
Total:	Summe aller gesendeten und empfangenen IP-Pakete während der Online-Verbindung
Invalid:	Anzahl der fehlerhaften (ungültigen) IP-Frames
Bytes	
Received:	Anzahl der empfangenen Daten-Bytes innerhalb eines IP-Frames
Sent:	Anzahl der gesendeten Bytes eines IP-Frames
Total:	Summe aller gesendeten und empfangenen Bytes auf IP-Ebene während der Online-Verbindung
Invalid:	Anzahl der fehlerhaften Bytes innerhalb eines IP-Datenpakets
Device IP:	IP-Adresse, die das *MD740-1* bei Verbindungsaufnahme ins GPRS-Netz vom Netz-Provider erhalten hat. Diese dynamische IP-Adresse wird dem Gerät zugewiesen und ist die IP-Adresse für eintreffende Datenpakete. Es ist davon auszugehen, dass dem *MD740-1* bei jeder erneuten Verbindungsaufnahme ins GPRS-Netz eine andere IP-Adresse (dynamische) vom Provider zugewiesen wird.

Seite Status Information

Klicken Sie auf der Startseite den Hyperlink *Status Information*, wenn Sie diese Seite einsehen wollen.
Diese Seite liefert Informationen über das GSM-Netz und den Netzbetreiber.

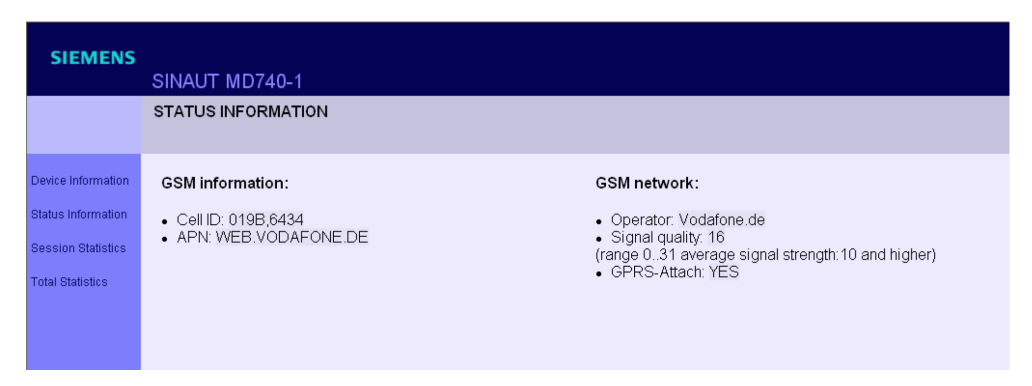


Abbildung 5-3

GSM-Information

Cell ID:	Die Cell ID ist eine eindeutige Kenn-Nummer für eine Zelle.
APN:	APN (Access Point Name) ist das Gateway aus dem GPRS-Netz zu anderen Netzen (z. B. Internet oder Intranet)

GSM-network

<table>
<tr><td>Operator</td><td colspan="2">Name des Netzbetreibers, (z.B. T-Mobile usw.).</td></tr>
<tr><td rowspan="7">Signal Quality</td><td colspan="2">Dieser Zahlenwert gibt die augenblickliche Signalqualität der Verbindung im GPRS-Netz an (Signal Quality).
Der gezeigte Wert für die Netzversorgung sollte sich in der unteren Tabelle wiederfinden.</td></tr>
<tr><th>Netzversorgung (Wert)</th><th>Bedeutung bzw. Signal</th></tr>
<tr><td>0</td><td>-113dBm oder schlechter</td></tr>
<tr><td>1</td><td>-111dBm</td></tr>
<tr><td>2...30</td><td>-109dBm bis -53dBm</td></tr>
<tr><td>31</td><td>-51dBm oder besser</td></tr>
<tr><td>99</td><td>nicht lesbar / unbekannt</td></tr>
</table>

GPRS-Attach:
Es wird mit *Yes* oder *No* angegeben, ob das *MD740-1* im GPRS-Netz eingebucht ist oder nicht.

Firmware-Update und Recovery 6

6.1 Update der Firmware des Modem-Teils

Das Modem-Teil des MD740-1 verfügt über einen integrierten FTP-Server (FTP = File Transfer Protocol). Mit diesem kann - sofern verfügbar - ein Update der Modem-Software ins MD740-1 geladen werden.

Benutzen Sie am besten ein FTP-Programm, um eine Verbindung zum FTP-Server des MD740-1 herzustellen.

Herstellen einer FTP Verbindung

Voraussetzung:

Die Firmware-Datei befindet sich auf dem Service-PC.

Vorgehensweise:

1. Zur Herstellung der Verbindung zum FTP-Server des MD740-1 genauso vorgehen wie beim Zugriff auf den Web-Server

   – lokal über die Service-Schnittstelle - siehe Kapitel 5.1

   – lokal über die Applikations-Schnittstelle (Buchse 10/100 BASE-T) - siehe Kapitel 5.2

   – von einem entfernten Rechner aus über das GPRS-Netz (netzabhängig) – siehe Kapitel 5.3.

2. Statt eines Web-Browsers starten Sie das FTP-Programm des Windows-Betriebssystems.

   Klicken Sie auf *Start, Ausführen*. Hinter *Öffnen* geben Sie ein:

   ftp 192.168.0.8 (oder die externe IP-Adresse, siehe Abschnitt 5.3).

   Sie werden dann nach dem Benutzernamen und dem Passwort gefragt.

Benutzername: **service**
Passwort: **service**

3. Nachdem die Verbindung hergestellt ist, können Sie die neue Firmware hochladen.

   Legen Sie mit Notepad (gehört zum Windows Zubehör) eine Datei mit folgendem Dateinamen an: **!cmdfile**
   Der Dateiname darf keine Dateinamenserweiterung wie z. B. .txt haben. Die erste Zeile in der Datei muss lauten:
   STORE MD740-1.bin
   (sofern „MD740-1.bin“ der Name der neuen Firmware-Datei ist). Dann Enter drücken.

   Hinter dem ftp>-Prompt geben Sie ein: **put MD740-1.bin**
   (sofern „MD740-1.bin“ der Name der neuen Firmware-Datei ist). Dann Enter drücken.

   Dann geben Sie hinter dem ftp>-Prompt ein: **put !cmdfile**
   Enter drücken.

   Nach dem Hochladen der Firmware- und der !cmdfile-Datei beginnt das Gerät, die neue Firmware zu installieren. Das kann bis zu 10 Minuten dauern. Danach vollzieht das Gerät einen Neustart.

4. Danach die Service-Verbindung abbauen:
   Hinter dem ftp>-Prompt geben Sie ein: **quit**
   Dann Enter drücken.
   Danach auch die Netzwerkverbindung zum Gerät beenden. Dazu das Verbindungssymbol in der Windows-Taskleiste drücken.

6.2 Recovery: Auf Werkseinstellungen zurücksetzen

Falls Sie keinen Zugriff mehr auf das MD740-1 haben sollten, weil Ihnen z. B. das Administratorpasswort verloren gegangen ist oder die Firewall-Regeln so gestellt sind, dass kein Konfigurationszugriff mehr möglich ist, können Sie über die SET-Taste das MD740-1 auf die Werkseinstellungen zurücksetzen. Die SET-Taste befindet sich auf der Vorderseite des Gerätes (siehe Kapitel 2).

Gehen Sie dazu wie folgt vor:

Die Versorgungsspannung muss angelegt sein.
Die SET-Taste gedrückt halten (z. B. mit einer aufgebogenen Büroklammer), bis die LED **Q** (das ist die mittlere LED) aufleuchtet.

Folge: Alle bestehenden Konfigurationseinstellungen werden dadurch gelöscht.

6.3 Update der VPN-Software

Die Versorgungsspannung muss angelegt sein.
Die SET-Taste gedrückt halten (z. B. mit einer aufgebogenen Büroklammer), bis die LED **C** (das ist die LED ganz rechts) aufleuchtet.

Weitere Informationen gibt es bei der Hotline.

Technische Daten 7

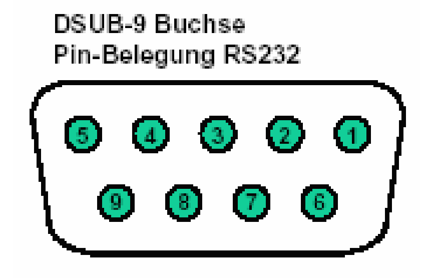
Schnittstellen	Applikations-Schnittstelle	10/100 Base-T (RJ45-Buchse) Ethernet IEEE802 10/100 Mbit/s
	Service-Schnittstelle	D-SUB-9 Buchse, PIN-Belegung RS232
Virtual Private Network	Protokoll	IPSec (Tunnel u. Transport Mode)
	Encryption:	3DES, AES, DES
	Paket Authentifizierung	MD5, SHA-1 Internet Key Exchange (IKE),
	Authentisierung	Pre-Shared Key (PSK), X.509v3 Zertifikate
	Weiteres	NAT-T, DynDNS, Dead Peer Detection (DPD)
Firewall		Stateful Packet Inspection Anti-Spoofing NAT (IP Masquerading) Port Forwarding
Weiteres		DNS Cache, DHCP Server, NTP, Remote Logging
Management		Web-basierte Administration
Verbindung	GPRS	Multislot class 10;
	Kodierungs-verfahren	CS-1, CS-2, CS-3, CS-4
Luftschnittstelle	GSM-Modul	GPRS / Quad Band
	GPRS	Bis zu 2 Uplinks / bis zu 4 Downlinks (max. 5 Slots)
	Sendeleistung	Quad Band; GSM 850 MHz: max. 2 Watt; GSM 900 MHz: max. 2 Watt; DCS 1800 MHz: max. 1 Watt; PCS 1900 MHz: max. 1 Watt
	Antennen-anschluss	Impedanz nominal: 50 Ohm, Buchse: SMA
Umwelt-bedingungen	Temperaturbereich	Betrieb: 0 °C bis +50 °C Lagerung: -25 °C bis +85 °C
	Luftfeuchtigkeit	0-95%, nicht kondensierend
Gehäuse	Bauform	Hutschienen-Gehäuse
	Material	Kunststoff
	Schutzart/-klasse	IP20
	Abmessungen	114 mm x 45 mm x 99 mm
	Gewicht	ca. 280g

Spannungs-versorgung	Leistungsaufnahme	typ. 8,0 W
	Eingangsspannung	18 - 30 VDC (24 VDC nominal)
	Eingangsstrom / Bestehende GPRS-Verbindung mit Datenaustausch	 I_n 450mA bei 18V (I_{Burst} 850mA), I_n 320mA bei 24V (I_{Burst} 800mA), 4,62ms Burst Wiederholrate
Prüfung/ Zulassung	CE	Ja
	R&TTE (GSM)	Ja
	GSM/GPRS-Modul	GCF; PTCRB konform
	EMV/ESD	EN 55024, EN 55022 Klasse A, EN 61000-6-2
	Elektrische Sicherheit	EN 60950
	ATEX	III 3 G EEx nA II T4 Ta=-20°C-50°C KEMA 03 ATEX 1229 X
	FM	CLI, DIV2, GP. A,B,C,D T4 Ta=-20°C-50°C CLI, Zone 2 IIC, T4 Ta=-20°C-50°C
	UL	E301826

Schnittstelle COM (Service)

Pin-Belegung:

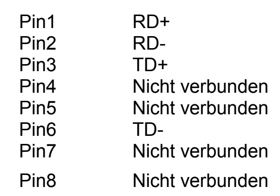
Signale RS232 (Signalrichtung DÜE)		
Pin1	Ausgang	DCD
Pin2	Ausgang	RXD
Pin3	Eingang	TXD
Pin4	Eingang	DTR
Pin5	Signal-Masse	GND
Pin6	Ausgang	DSR
Pin7	Eingang	RTS
Pin8	Ausgang	CTS
Pin9	Ausgang	RI



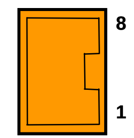
Pin-Belegung Schnittstelle 10/100 BASE-T

Signale (Signalrichtung DÜE)

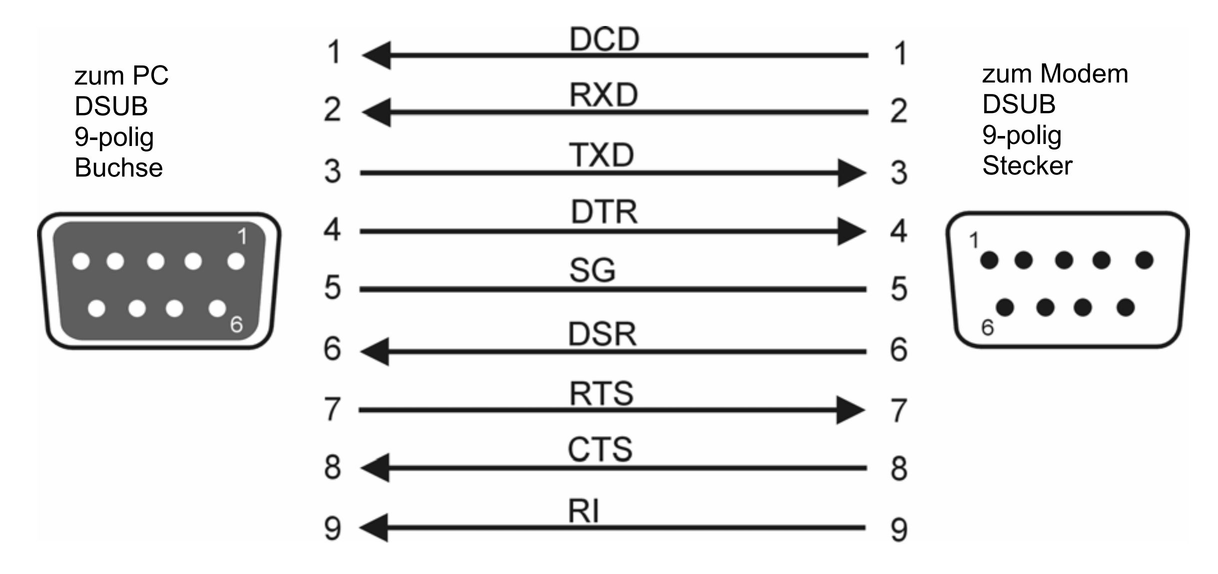
RJ45-Buchse - Ethernet



Pin1	RD+
Pin2	RD-
Pin3	TD+
Pin4	Nicht verbunden
Pin5	Nicht verbunden
Pin6	TD-
Pin7	Nicht verbunden
Pin8	Nicht verbunden



Modemkabel für Service Interface



Die Leitung RI ist optional.

Glossar

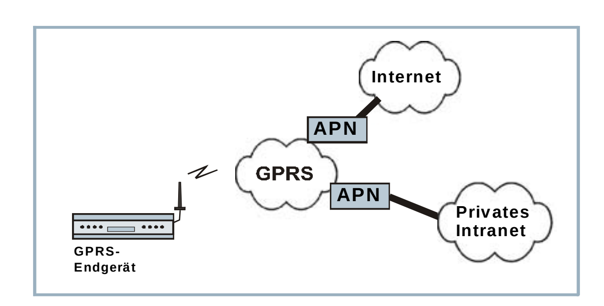
8

AES

Advanced **E**ncryption **S**tandard. Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit. 1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

APN (Access Point Name)

(Zugriffspunktname). Netzübergreifende Verbindungen, z. B. vom GPRS-Netz ins Internet, werden im GPRS-Netz über sogenannte APNs hergestellt.



Ein Endgerät, das eine Verbindung über das GPRS-Netz aufbauen will, gibt durch Angabe des APN an, mit welchem Netz es verbunden werden will: Internet oder privates Firmennetz, das über Standleitung angeschlossen ist.
Der APN bezeichnet den Übergabepunkt zum anderen Netz. Er wird dem Benutzer vom Netzbetreiber mitgeteilt.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen

Kommunikationspartnern, gegeben.

Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, dass die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.

Asymmetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwändige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das/der vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.
Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D.h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

Datagramm

Beim Übertragungsprotokoll TCP/IP werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:
1. IP-Header
2. TCP-/UDP-Header
3. Daten (Payload)

Der IP-Header enthält:
- die IP-Adresse des Absenders (source IP-address)
- die IP-Adresse des Empfängers (destination IP-address)
- die Protokollnummer des Protokolls der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
- die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:
- Port des Absenders (source port)
- Port des Empfängers (destination port)
- eine Prüfsumme über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology

(NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Das es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.
DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.
3DES ist eine Variante von DES. Es arbeitet mit 3 mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol). Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einem Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.
Soll ein lokaler Rechner über das Internet erreichbar sein, muss seine Adresse der entfernten Gegenstelle bekannt sein. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat ein Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).
Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.xyz.abc.de. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.
Wenn jetzt ein entfernter Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der entfernte Rechner den Hostnamen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum entfernten Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.
Allen Internetadressen liegt prinzipiell dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz, aufgebaut.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.
Eine IP-Adresse besteht aus 2 Teilen: der Netzwerk-Adresse und der

Host-Adresse.
Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorien Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:

	1. Byte	2. Byte	3. Byte	4 Byte
Class A	Netz-Adr.	Host-Adr.		
Class B	Netz-Adr.		Host-Adr.	
Class C	Netz-Adr.			Host-Adr.

Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	Bytes für die Netz-Adresse	Bytes für die Host-Adresse
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

IPsec

IP security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPSec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA), der Security-Parameter-Index (SPI) und der Internet Key Exchange (IKE).
Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. Transport Mode oder Tunnel Mode.
Im Transport Mode wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPSec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host-zu-Host-Verbindung geeignet.
Im Tunnel Mode wird dem gesamten IP-Datagramm ein IPSec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.
Der Tunnel Mode findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrecke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als IP-Masquerading bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über den NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.
Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.
Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den IP- und den TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzten Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.
Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Port-Nummer

Das Feld Port-Nummer ist ein 2 Byte großes Feld in UDP- und TCP-Headern. Die Vergabe der Port-Nummern dient der Identifikation der verschiedenen Datenströme, die UDP/TCP gleichzeitig abarbeitet. Über diese Port-Nummern erfolgt der gesamte Datenaustausch zwischen UDP/TCP und den Anwendungsprozessen. Die Vergabe der Port-Nummern an Anwendungsprozesse geschieht dynamisch und wahlfrei. Für bestimmte, häufig benutzte Anwendungsprozesse sind feste Port-Nummern vergeben. Diese werden als Assigned Numbers bezeichnet.

PPPoE

Akronym für Point-to-Point Protocol over Ethernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für Point-to-Point Tunneling Protocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Private Key (privater Schlüssel), Public Key (öffentlicher Schlüssel); Zertifizierung (X.509)

Bei asymmetrischen Verschlüsselungsalgorithmen werden 2 Schlüssel verwendet: ein privater (*Private Key*) und ein öffentlicher (*Public Key*). Der öffentliche Schlüssel dient zum Verschlüsseln von Daten, der private Schlüssel zum Entschlüsseln.
Der öffentliche Schlüssel wird vom zukünftigen Empfänger von Daten denen zur Verfügung gestellt, die die Daten verschlüsselt an ihn versenden werden. Der private Schlüssel ist nur im Besitz des Empfängers. Er dient zum Entschlüsseln der empfangenen Daten.
Zertifizierung:
Damit der Benutzer des (zum Verschlüsseln dienenden) öffentlichen

Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung: Die Überprüfung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Absenders mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Absender beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Prüfung signiert die CA den öffentliche Schlüssel des Absenders mit ihrer (digitalen) Unterschrift. Es entsteht ein *Zertifikat*.
Ein X.509-Zertifikat stellt eine Verbindung zwischen einer Identität in Form eines 'X.500 Distinguished Name' (DN) und einem öffentliche Schlüssel her, die durch die digitale Signatur einer X.509 Certification Authority (CA) beglaubigt wird. Die Signatur - eine Verschlüsselung mit dem Signaturschlüssel - kann mit dem privaten Schlüssel überprüft werden, die die CA dem Zertifikatsinhaber aushändigt.

Protokoll, Übertragungs-protokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen". Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutzte Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP. TCP/IP ist der Oberbegriff für alle auf IP aufbauenden Protokolle.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Anti-Spoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.
Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 134.76.0.0. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).

Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die *Subnetz-Maske*. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu "borgen", um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das

eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/Internet Protocol

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.
IP ist das Basisprotokoll.
UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.
TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.
UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.
Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).
ICMP baut auf IP auf und enthält Kontrollnachrichten.
SMTP ist ein auf TCP basierendes E-Mail-Protokoll.
IKE ist ein auf UDP basierendes IPsec-Protokoll.
ESP ist ein auf IP basierendes IPsec-Protokoll.
Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.
(→ Datagramm)

VPN (Virtuelles Privates Netzwerk)

Ein **V**irtuelles **P**rivates **N**etzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

X.509 Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.

Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels

beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguished Name (DN)), erlaubte Verwendungszwecke usw. und der Signatur der CA.

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509 Zertifikate kommen z.B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.